Installation and Reference Guide

hp StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition

Product Version: 3.0C

Third Edition (February 2004)

Part Number: AA–RU7VD–TE

This guide describes the HP StorageWorks Secure Path for Linux and Linux Workgroup edition software. It includes information about Secure Path technology, installation procedures, and management commands.

Printed in the U.S.A.

Secure Path v3.0C for Linux and Linux Workgroup Edition Installation and Reference Guide
Third Edition (February 2004)
Part Number: AA–RU7VD–TE

contents

about this guide

This installation and reference guide provides information to help you:

- Understand Secure Path Technology
- Determine hardware and software prerequisites
- Install Secure Path software
- Manage Secure Path using `spmgr`
- Contact technical support for additional assistance

"About this Guide" topics include:

Overview

This section covers the following topics:

Intended audience

This book is intended for use by system administrators who are experienced with the following:

- Linux operating systems
- EVA5000
- EVA3000
- RA/MA8000
- ESA/EMA12000
- MSA1000

Related documentation

In addition to this guide, HP provides the *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Release Notes*.

Conventions

Conventions consist of the following:

- Document conventions
- Text symbols
- Equipment symbols

Document conventions

This document follows the conventions in Table 1.

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Getting help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP technical support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP storage web site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP authorized reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

Secure Path Technology

1

HP StorageWorks Secure Path is a server-based software product that enhances StorageWorks RAID array storage systems by providing automatic path recovery from server-to-storage system connection failures. Secure Path supports multiple I/O paths between host and storage, which improves overall data availability. If any component in a path between host and storage fails, Secure Path redirects pending and subsequent I/O requests to an alternate path.

This chapter provides the following Secure Path information:

Overview

Note: You must have root privileges to perform Secure Path installation or spmgr commands

Secure Path is a high-availability software product that manages and maintains continuous data access to the following StorageWorks storage systems:

- RA8000
- ESA12000
- MA8000
- EMA12000
- EVA5000
- EVA3000
- MSA1000

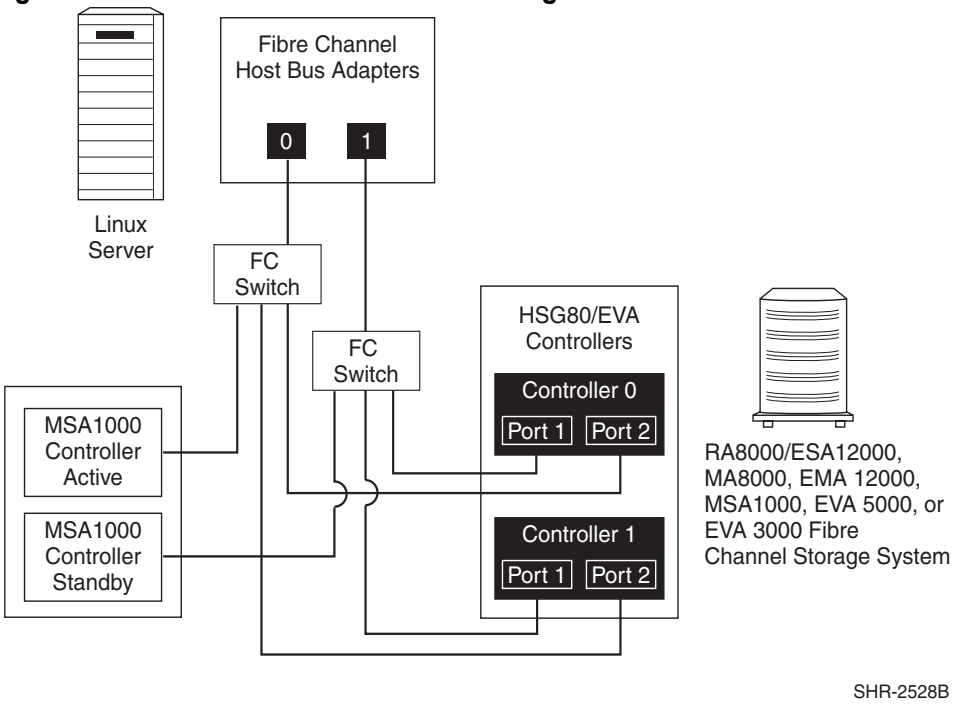
Secure Path eliminates the RAID controller, HBA, and interconnect hardware (cables, switches, and connectivity devices) as single points of failure in the I/O path.

By using redundant hardware and advanced RAID technology, Secure Path enhances fault tolerance and storage system availability by providing automated failover capability.

Redundant physical connections define separate physical *paths* in a Secure Path hardware configuration. Each path originates at an HBA port on a server, and ends at a unique RAID controller port in the storage system.

Figure 1 illustrates basic Secure Path hardware configurations. The physical connections define two separate paths. Each path originates at a unique SAN host bus adapter on a Linux server and ends at a port on a separate RAID controller on the storage system.

Figure 1: Basic Secure Path Fibre Channel configuration



For HSG80, EVA5000, and EVA3000 storage systems, Secure Path enables dual StorageWorks RAID controllers to operate in an active/active LUN ownership implementation, referred to as dual-redundant multiple-bus mode. Multiple-bus mode allows each controller to process I/O independently of the other controller under normal operation. A path consists of a unique connection from adapter to device. I/O is active on one controller at a time, and storage units (LUNs) may be moved between paths and controllers using the Secure Path Management Tool `spmgr`.

For MSA1000 storage systems, dual StorageWorks RAID controllers operate in an Asychronous LUN presentation implementation, where one MSA1000 controller actively processes I/O and an alternate controller remains on standby.

Secure Path takes advantage of the Preferred Path attribute. For the HSG80/HSV110/HSV100 available storage units, a path may be preferred for each controller by setting the Preferred Path attribute.

For the MSA1000, storage units are available to the active controller. The MSA1000 has a default preferred controller, which is used for access at storage system boot time. During runtime, storage units may be moved between paths at any time through the use of the Secure Path Management utility. On HSG80/HSV110/HSV100 RAID storage systems, storage units may also be accessed on each controller through either of two available ports.

The Secure Path software detects the failure of I/O operations on a failed path and automatically reroutes traffic to other available paths. Secure Path software will seek alternate paths through available SAN switches, controllers, controller ports, and host bus adapters. Path failover is completed seamlessly, without process disruption or data loss.

Following warm swap or replacement of a failed adapter, cable, controller, or attached components, storage units can be restored to their original path using the Secure Path Management utility.

To protect against drive failure in a Secure Path environment, storage units can be configured using configuration tools. Fault tolerance is the ability to recover from hardware problems without interrupting the server's performance.

High availability configurations for HSG80, HSV110, and HSV100 include RAID levels 0+1, 1, or 5.

MSA1000 High availability configurations include RAID levels 0+1, 4, or 5.

Features

Secure Path provides the following features:

- Allows StorageWorks dual-controller RAID systems and host servers equipped with multiple HBAs redundant physical connectivity along independent Fibre Channel fabric paths
- Monitors each path and automatically reroutes I/O to a functioning alternate path if a component failure occurs
- Determines the availability of storage units and physical paths through path verification diagnostics
- Monitors and identifies failed paths and failed over storage units
- For the HSG80, HSV110 and HSV100 storage systems, Secure Path facilitates static Load Balancing, which allows manual movement of devices between controllers
- Automatically restores failed over storage units to repaired paths with Auto-Restore capability enabled
- Implements antithrash filters to prevent failover/restore effects caused by marginal or intermittent conditions
- Exploits the potential for improved data throughput and increased bandwidth using dual RAID controllers configured in multiple-bus mode operation with Load Balancing capability enabled. This feature applies to the HSG80, HSV110, and HSV100 storage systems only
- Detects failures reliably without inducing false or unnecessary failovers
- Implements failover/restore actions transparently without disrupting applications

Software components

This section describes the Secure Path Software Kit for Linux software components.

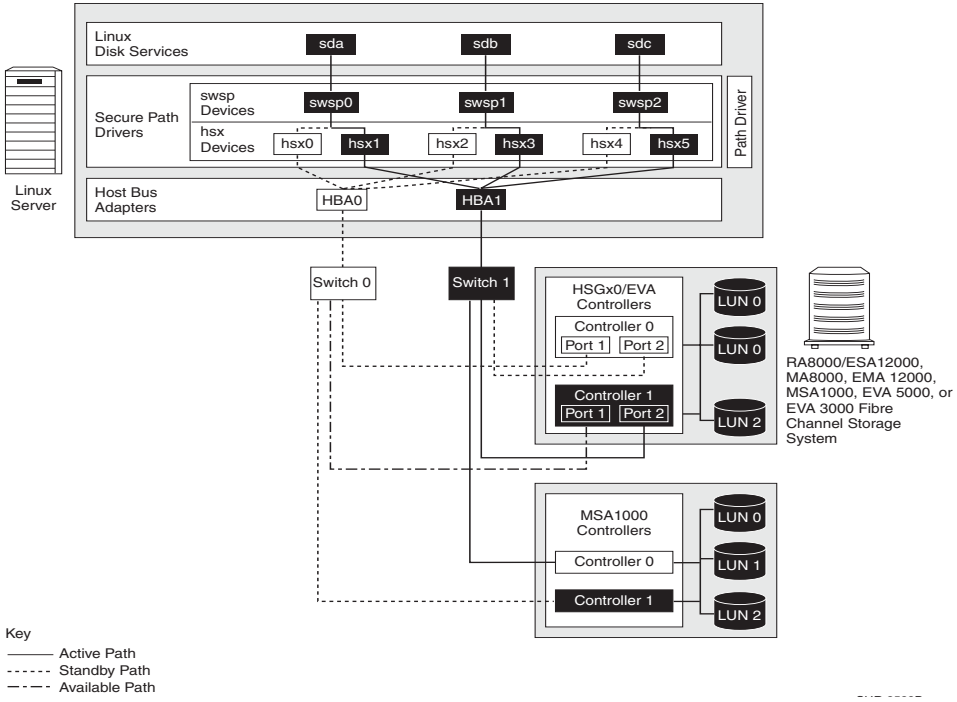
Drivers

Secure Path drivers consists of the following three modules:

- `swsp_mod.o module`—A virtual HBA driver that takes requests from Linux SCSI subsystem mid-layer and passes the requests to the `hsx_mod.o` module with the help of the `path_mod.o` modules.
- `path_mod.o module`—Required to allow the `hsx` and `swsp` modules to communicate in the kernel.
- `hsx_mod.o module`—Acts as a target driver but never registers itself with the SCSI mid-layer. It manages all the paths for logical LUNs while `swsp_mod.o` manages the failover for paths.

Figure 2 illustrates the driver model structure

Figure 2: Driver model structure.



Agent

The Secure Path agent (`spagent`) is a daemon process that provides an interface for Secure Path applications and utilities to communicate to the multipath drivers. The `spagent` also provides notification of path change events through e-mail. The `spagent` is not required to be running for Secure Path drivers to configure and provide full failover functionality. However, it must be running if e-mail event notification is desired. The only supported method to start and stop the Secure Path agent is the `spinit` script.

Management tools

The Secure Path Manager (`spmgr`) is a command line application that allows you to monitor and manage Secure Path devices and to change the configuration settings of the drivers. Refer to "Managing Secure Path" on page 57 for a complete description of `spmgr` commands.

Note: You must have network services running in order for *spmgr* to communicate with *spagent*.

Controller ownership

Storage systems that are multiple-bus capable generally contain a pair of redundant controllers and support one of the following basic operational models:

- The MSA1000 uses the active/passive operational model. In the active/passive model, all storagesets are assigned ownership to one controller of the pair for I/O processing. The other controller is standby and is available as a substitute in case of failure on the original.
- The HSG80, EVA5000, and EVA3000 use the modified active/active operational model. In the active/active model, I/O processing may be routed through both controllers simultaneously, providing better performance in addition to high availability. The RAID arrays supported by Secure Path implement a modified version of the active/active model. Although I/O can be processed simultaneously by both controllers, any given storageset is *owned* or online to a host through only one controller.

  Ownership of a storageset may be transferred to the other controller at any time through a host-initiated command sequence. However, because the ownership transfer results in controller cache flushing and I/O wind down, the storageset may become inaccessible for a period of several seconds. Arbitrary ownership transfers are never automatically initiated by Secure Path and should be avoided.

Note: Secure Path automatically retries I/O requests that terminated in error due to ownership transfers. It also queues new I/O requests until the ownership transfer has completed, to ensure data integrity.

Path definition

Within Secure Path, a path is defined as the collection (configuration) of physical interconnect components including HBAs, switches, cables, RAID controllers, and the ports on the controllers. Because the Secure Path driver component is positioned between the HBA driver and the system SCSI disk driver, the Secure Path driver can only distinguish physical paths when elements of the SCSI equivalent address are different.

Some configurations include multiple switches within a fabric, with the switches connected by one or more interswitch links. Secure Path cannot detect these paths and cannot manage them. While these interswitch paths provide an additional level of redundancy within the fabric, their management is handled directly within the switch. Refer to the documentation received with your switch hardware for more information about interswitch link routing and failover policies.

Secure Path automatically sets the path state, and reflects the status of the current actual path. Because of path failures, the currently active path may be different from what you expect. See Table 8 on page 62 for a list and description of path states and attributes.

Secure Path operation

Path failover occurs automatically when a selected set of error conditions is detected. Secure Path normally performs path failover only when user I/O is active or if path verification is enabled. However, it is possible for Secure Path Manager to show some units with a common failed path in the failover state, while other units remain accessible through that path. Units remain in the failed path if there is no I/O or until they are polled.

For the HSG80, EVA5000, and EVA3000, failover follows a hierarchy, conditioned by the state of Load Balancing, as described below. Secure Path does not change the mode of *Preferred* paths in failover situations, so you can restore original path assignments after making repairs.

- Load Balancing disabled:

  When a failure occurs, Secure Path marks the path *Failed* and switches to the next *Available* path connected to the same controller, if there is one.

  If there is no *Available* path on the same controller, Secure Path attempts to move the device to a *Standby* path on the other controller.

- Load Balancing enabled:

  When a failure occurs, Secure Path marks the affected path as *Failed*. This removes it from the list of usable paths for the storageset.

  — If no *Active* paths remain for the device, Secure Path activates an *Available* path on the same controller, if one exists.

  — If no *Available* paths remain on the same controller, Secure Path attempts to move the device to a *Standby* path on the other controller.

Restore options

Secure Path lets you set the path Restore option to *Manual* or *Automatic*.

- In Manual mode, you must enter a management utility command to restore devices to their preferred path. The operation is performed even if system I/O is in process to the selected device.
- In Automatic mode, Secure Path tests a failed path at fixed intervals if I/O is in process for the affected device. If the path appears to be viable, and the path is set as *Preferred*, the path state is set to *Active* and I/O will again be routed through this path.

Load balancing

Secure Path supports the Load Balancing attribute. When enabled, Load Balancing allows multiple paths between a host and a specific storageset to be used in a round robin fashion. Using multiple paths spreads the load across all components in the RAID storage system.

Load Balancing may not be used in environments that use device reservations as a lock mechanism because the RAID array controllers enforce reservations on a per-port basis.

Load Balancing requires a Fibre Channel configuration that results in at least two paths per controller from the host node to the storage system. While this can be accomplished with several different physical configurations, maximum performance potential is achieved when all ports of the RAID storage system are used.

When Load Balancing is enabled, the Secure Path driver causes all paths to the owning controller to be marked *Active* by default. This is true when the following conditions occur:

- A host boots up
- Secure Path fails over a storageset from one controller to the other
- For the EVA3000/EVA5000 or HSG80, you can manually move a selected storageset between controllers using the Secure Path management utility, `spmgr`.

Path verification

When enabled with `spmgr`, Path Verification causes Secure Path to periodically test the status of all paths to all storagesets and marks them *Available*, *Failed, Active*, or *Standby*. Path Verification does not test paths that are in a *Quiesced* state.

Path verification is useful for detecting failures that affect overall path redundancy, before they affect failover capability. If an *Active* path fails path verification, failover occurs. If a path fails path verification, its state will change from *Available* to *Failed*.

If a path marked *Failed* passes path verification, the path state is set to *Available* if it is on the *Active* controller and *Standby* if it is on the *Standby* controller. If Auto-Restore is enabled, the path becomes *Active* only if the path is on the *Active* controller and it is marked *Preferred*.

Path management behavior summary

Table 2 provides a summary of the path management behavior of Secure Path.

Table 2: Path management behavior summary

Feature	Behavior/Action
Startup	1. Chooses the *Preferred* path to the controller on which the LUN is online. 2. Marks the *Preferred* path *Active.* If no path is marked *Preferred*, select one and make it the *Active* Path.
Active Path Failure	■ Marks the *Active* path as *Failed* and fails to the *Available* path. ■ Redirects I/O through available paths. ■ If there are no *Available* paths, failover occurs to a *Standby* path on the other controller.
Available or Standby Path Failure	■ Performs path verification ■ Marks failed path as *failed*
Path Repaired	■ Marks the path *Available* or *Standby* depending on which controller the device is currently online to. ■ If Auto-Restore is enabled, and the path is preferred, then that path is marked *Active*.

Table 3 shows the default values with which Secure Path is enabled.

Table 3: Secure Path installation default values

Parameter	Default value
Autorestore	off
Load Balancing (HSG80, EVA5000, EVA3000 only)	off
Path Verification	on
Verification period	30 seconds
Preferred paths	None
Console event log messages	Critical
Syslog event log messages	Critical, Warning
Mail event log messages	Logging is disabled(0) Critical, Warning, and Informational (3)
Mail event log e-mail	Enabled to send to the root account

Use the `spmgr` utility to customize your configuration. Refer to "Managing Secure Path" on page 57 for more information on `spmgr` customization.

Hardware Setup

2

This chapter provides the following Secure Path hardware setup information:

Hardware setup overview

The following procedure presents an overview of the hardware setup:

1. Ensure that all users have logged off the server and all array file systems have been backed up and unmounted, prior to setting up your hardware.
2. Verify that all the following hardware and software prerequisites have been met:
   - Supported Host Bus Adapters (HBAs) must be installed and working properly.
   - Supported version of Linux and with all required patches loaded.
   - Supported version of the Solution Software Kit is installed.

Note: Refer to the *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Release Notes* for all hardware and software prerequisites.

---

3. Configure your StorageWorks RAID array.
4. Cable your HBAs, switches, and storage, making sure that the configuration is valid.

This guide describes only one basic Secure Path configuration. Many more valid configurations are possible; however, they are not documented here. Therefore, before installing Secure Path on a new or existing Fibre Channel (FC) configuration, first review the *HP StorageWorks SAN Design Reference Guide* found on the HP web site. The guide familiarizes you with various high availability connection layouts for FC devices and cabling.

For the most current reference guide, visit the HP web site at http://hp.com/country/us/eng/prodserv/storage.html.

Required components

Before installing Secure Path software, verify that you have received the Secure Path software kit and the FC hardware that you ordered for this installation. If you are missing any components, please contact your account representative or call the HP Customer Services Hotline at 1-800-354-9000. The basic requirements for Secure Path operation and version information are listed in the *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Release Notes* that you received with this Secure Path v3.0C for Linux release.

Installing and configuring the storage systems

This section describes the steps required for installing and configuring RAID systems and Linux servers for Secure Path operation in fabric (FC-SW) mode. This section is divided into three parts, one for EVA5000/EVA3000 storage systems, one for setting up HSG80-based storage systems, and one for setting up the MSA1000-based storage systems.

Before proceeding, you should have all Fibre Channel adapters installed in your Linux server. If required, power down your server and install the Fibre Channel adapters per the adapter installation instructions. Reboot your server and ensure that the adapters are functioning before proceeding.

If you are using EVA5000/EVA3000 storage, follow the procedure described in "Configuring StorageWorks enterprise virtual arrays" on page 31for setup instructions.

If you are using HSG80-based storage, follow the procedure described in "Configuring StorageWorks MA8000/EMA12000 RAID arrays" on page 33 for setup instructions.

If you are using MSA1000-based storage, follow the procedure described in the documentation that came with your controller for setup instructions.

For instructions on connecting your storage to your server, and preparing to install Secure Path, follow the procedure described in "Connecting storage to the server" on page 39.

Configuring StorageWorks enterprise virtual arrays

This section provides the steps required to install and configure HSV110/HSV100-based storage arrays.

Before beginning, collect and record the following host information:

- LAN name of the host
- Host IP address
- A list of the Fibre Channel Adapter World Wide Names that will be configured for Secure Path

Access the Command View EVA management appliance from a supported web browser, such as Internet Explorer or Netscape Navigator.

Before your host servers can use the virtual disks, ensure that you have the following items completed:

Note: Refer to the for HP StorageWorks Command View EVA online Help for information about these procedures. All of these procedures need to be completed for your host to use the virtual disks.

1. **Initialize the storage system and create disk groups**. When you first view the EVA5000/EVA3000 from the Command View EVA software, the storage pool is presented as *uninitialized storage*. Follow documented procedures for initializing your storage systems and creating disk groups in the *HP StorageWorks Command View EVA Enterprise Virtual Array Getting Started Guide.*
2. **Add the host to the storage system**. Before the host can use the storage system's virtual disks, the host must be known to the storage system. Adding the host creates a path from the storage system to one host adapter.
3. **Add ports to all host adapters**. From the Host Properties page, choose **Add Port** to add connections to the remaining HBA host adapters.
4. **Create and present virtual disks to the host**. Follow documented procedures for creating your virtual disk family and presenting the disks to the host in the *HP StorageWorks Command View EVA Enterprise Virtual Array Getting Started Guide.*

Several options are available for selecting a path preference and mode for a virtual disk. To optimize Load Balancing the load should be evenly distributed between controller A and controller B. The boot default selected controller may be chosen by setting the controller *Preferred path/mode*. It is recommended that either **Path A - Failover only** or **Path B - Failover only** be used. This mode allows Secure Path to control a restore to the original controller following a controller failure and replacement.

Note: **Path A - Failover/failback** and **Path B - Failover/failback** are not supported on Secure Path for Linux. That feature is designed for operating systems that cannot run Secure Path.

Configuring StorageWorks MA8000/EMA12000 RAID arrays

This section provides the steps to install and configure HSG80-based storage arrays.

Caution: If you are installing Secure Path on an existing RAID storage system, stop **all** I/O to the RAID system and skip steps 1 and 2 below. For each RAID system in a production environment being converted to Secure Path operation, also make sure that all users have logged off the Linux servers. Follow normal procedures to back up the storage systems before proceeding.

1. Unpack the RAID system and install the PCMCIA cards in the controllers.
2. Power on the RAID system. Allow the cache batteries to charge, if necessary, before proceeding.
3. Establish a serial connection to the RAID storage system, and use the CLI utility to configure the RAID system and create storagesets, as required.

Caution: Before proceeding, allow initialization of the storagesets to complete.

Note: Secure Path installation requires that at least one LUN be configured on the RAID storage system, but a complete disk/device configuration is strongly recommended. Additionally, the units must be visible to at least two paths from the Linux server.

4. Verify the configuration of the RAID system by entering either of the following commands:

   ```
   CLI > show this_controller
   CLI> show other_controller
   ```

   An example of the controller output (with reference line numbers appended) follows:

```
Controller:                                                    1.
        HSG80 ZG90305234 Software V86F-4, Hardware E08         2.
        NODE_ID          = 5000-1FE1-0000- 8920                3.
        ALLOCATION_CLASS = 0                                   4.
        SCSI_VERSION     = SCSI-3                              5.
        Configured for MULTIBUS_FAILOVER with ZG90811309       6.
            In dual-redundant configuration                    7.
        Device Port SCSI address 6                             8.
        Time: 01-AUG-2000  09:39:19                            9.
        Command Console LUN is 0                              10.
Host PORT_1:                                                  11.
        Reported PORT_ID = 5000-1FE1-0000-8923                12.
        PORT_1_TOPOLOGY = FABRIC (fabric up)                  13.
       Address          = 021000                              14.
Host PORT_2:                                                  15.
        Reported PORT_ID = 5000-1FE1-0000-8924                16.
        PORT_2_TOPOLOGY = FABRIC (connection down)            17.
NOREMOTE_COPY                                                 18.
Cache:                                                        19.
        128 megabyte write cache, version 0012                20.
        Cache is GOOD                                         21.
        No unflushed data in cache                            22.
        CACHE_FLUSH_TIMER = DEFAULT (10 seconds)              23.
```

```
Mirrored Cache:                                          24.
        128 megabyte write cache, version 0012           25.
        Cache is GOOD                                    26.
        No unflushed data in cache                       27.
Battery:                                                 28.
        NOUPS                                            29.
        FULLY CHARGED                                    30.
        Expires:                        16-DEC-2001      31.
```

a. Configure the RAID system controllers for Multiple-bus Failover Mode, if the controllers are in Transparent Failover Mode (see line 6 of the example controller output). This procedure is documented in "Changing from Transparent Failover to Multiple-bus Failover mode" on page 108.

   In Transparent Failover Mode, under fabric configuration, both left-hand ports share the same WWPN. Similarly, both right-hand ports share the same WWPN. Set the preferred path, if desired, for each storage unit to specify the controller that the unit will use upon the RAID system boot time as follows:

   Enter the following command to obtain a list of all units defined in the RAID storage system:

   ```
   CLI> show units full
   ```

An example of the show units output follows:

```
D11                                             DVGRPR0    (partition)
   LUN ID:      6000-1FE1-0000-8920-0009-9030-5234-006E
   NOIDENTIFIER
   Switches:
    RUN                   NOWRITE_PROTECT       READ_CACHE
     READAHEAD_CACHE         WRITEBACK_CACHE
     MAXIMUM_CACHED_TRANSFER_SIZE = 32
   Access:
           ALL
   State:
     ONLINE to this controller
     Not reserved
     NOPREFERRED_PATH
   Size:              8533749 blocks
   Geometry (C/H/S): (1680 / 20 / 254)
```

As shown in this example, the state of the unit is online to `this_controller` and no preferred path has been assigned.

b. Enter one the following commands to specify the preferred path for each of the units:

```
CLI> set (unit #) preferred_path = this_controller
```

- or -

```
CLI> set (unit #) preferred_path = other_controller
```

Example:

```
CLI> set d11 preferred_path = other_controller
```

c. Enter the following CLI commands to transition the units to the preferred path:

```
CLI> shutdown other_controller
CLI> shutdown this_controller
```

d. Restart the controllers by pressing RESET on each controller at the same time.

Configuring StorageWorks Modular Smart Array 1000

This section provides the steps required to install and configure MSA1000-based storage arrays.

1. Verify that you have a supported server with a supported Linux operating system installed prior to configuring your MSA1000.
2. Verify that a supported Fibre Channel Host Bus Adapter (HBA) is installed.
3. Install the MSA1000 Storage System in a rack, following instructions found in your rack documentation.
4. Connect the Fibre Channel HBA and the Fibre Channel switches or hub by using the appropriate length of Fibre Channel cable.
5. Apply power to all the MSA1000 controllers.
6. Insert the Modular Smart Array 1000 Support Software CD in your CD-ROM drive.
7. If your server does not automatically mount your CD-ROM, you must manually mount the CD-ROM. For example:

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```

8. Change directories using the following command:

   ```
   # cd /mnt/cdrom/LINUX
   ```

9. Install RPM based on the OS version that this system is running. For example:

   ```
   # rpm -ivh qla2x00-x.x.x-x.Redhat-2-7.i386.rpm
   ```

   RPM installs some system changes necessary for the MSA1000 storage system and installs the HBA driver.

10. Change directories using the following command:

    ```
    # cd /LINUX/onacuxe
    ```

11. Issue the following command to install `cpqacuxe`:

    ```
    # rpm –ivh cpqacuxe-XXX.i386.rpm
    ```

Note: Replace X with the current version of the *cpqacuxe* for Linux or the current version of *qla2x00*.

---

12. Start the daemon by executing the following command:

    ```
    # /usr/sbin/cpqacuxe
    ```

13. Click **Netscape** and connect to http://127.0.0.1:2301.

Refer to the documentation supplied in your Modular Smart Array 1000 Setup and Management kit for further details.

Note: Before Installing Secure Path for Linux, you must enable the proper host mode setting using the ACU utility. Refer to the ACU documentation for steps to change the host mode.

Connecting storage to the server

This section describes how to connect configured storage to your server. For more information on supported configurations, access the HP web site at: http://hp.com/country/us/eng/prodserv/storage.html.

1. Cable the Fibre Channel adapter and the RAID storage system controllers to the SAN Switches and HBAs, as shown in Figure 3.
2. Choose from the following options:
   a. Proceed to "Installing Secure Path Software" on page 43 to install Secure Path if all the storage systems that you are configuring are EVA5000/EVA3000 or RA8000/EMA12000 arrays in SCSI-3 CCL mode.
   b. Map WWPNs to targets as shown in step 3 through step 5 if you have any HSG80-based storage using SCSI-3 CCL mode.

Note: You must map WWPNs before installing Secure Path as described in "Installing Secure Path Software" on page 43.

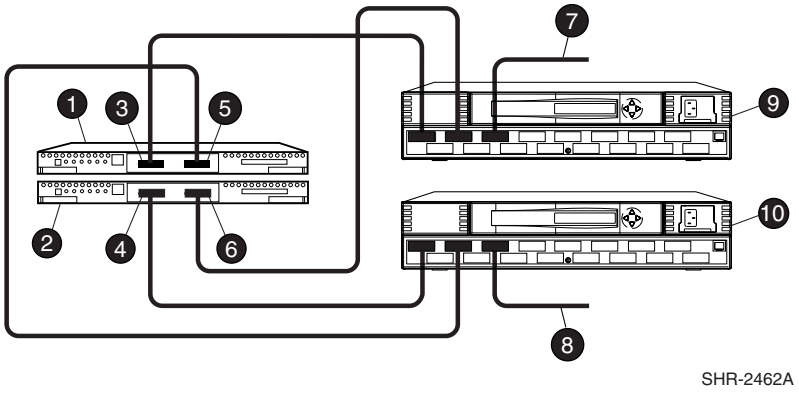


Figure 3: Cabling two RAID controllers and two SAN switches

❶ Top Controller	❻ Bottom Controller, port 2 (to host via top switch)
❷ Bottom Controller	❼ FC cable to host bus adapter A
❸ Top Controller, port 1 (to host via top switch)	❽ FC cable to host bus adapter B
❹ Bottom Controller, port 1 (to host via bottom switch)	❾ SAN Switch (top)
❺ Top Controller, port 2 (to host via bottom switch)	❶❿ SAN Switch (bottom)

3. If you do not have a supported version of the StorageWorks Solution Software you will need to install it now. Refer to the *HP StorageWorks Secure Path v3.0C for Linux and Linux Workgroup Edition Release Notes* for supported hardware and software. Also see the instructions provided in the Solutions Software kit.

4. Verify that the correct WWPNs have been mapped to targets using the following command. The correct WWPN is shown in the output displayed on line 2.

Note: This example shows only partial output from the command.

```
CLI> show this
 Host PORT_1:                                                    1.

         Reported PORT_ID = 5000-1FE1-0000-8923                  2.

         PORT_1_TOPOLOGY = FABRIC (fabric up)                    3.

 Address          = 021000                                       4.

 Host PORT_2:                                                    5.

         Reported PORT_ID = 5000-1FE1-0000-8924                  6.

         PORT_2_TOPOLOGY = FABRIC (fabric up)                    7.
```

After you install the Solution Software and the WWPNs have been mapped to targets, you are prompted to reboot your system with the reconfigure flag.

Note: Refer to the *Solution Software for Linux – Installation Reference Guide* for detailed Solution Software configuration information, including fabric instances of the WWPNs.

5. Use the following command to reboot your system:

```
# reboot
```

6. Use the following command sequence after rebooting to check the RAID storage system to ensure that the connection operating system setting is Linux:

   a. Enter the `show connection` command to inspect the connection settings:

```
CLI> show connection

Connection                                                    Unit
Name      Operating system Controller Port Address Status
Offset

!NEWCON021000 Linux         THIS       1    000001  OL this  0

   HOST_ID=1000-00E0-6940-123C  ADAPTER_ID=2000-00E0-6940-123C

!NEWCON031000 Linux         OTHER      1    000001  OL other 0

   HOST_ID=1000-00E0-6940-11A8   ADAPTER_ID=2000-00E0-6940-11A8
```

   b. Enter the following command to set the operating system:

```
CLI> set [connection name] operating_system = Linux
```

   c. Perform one of the following actions:

      — If a RAID storage system is shared (accessed by more than one server), HP recommends the use of Selective Storage Presentation where both `offset` and `enable_access_path` be applied to each connection and unit on the RAID system by entering the following command:

```
CLI > set [connection name] unit_offset = offset_value
```

      — For installations that do not have shared storage, an offset of 0 is recommended as follows:

```
CLI > set [connection name] unit_offset = 0
```

   d. Set the `enable_access_paths`:

```
CLI > set Dn disable_access_path = all

CLI > set Dn enable_access_path = connection_name,
connection_name

CLI > restart other_controller

CLI > restart this_controller
```

The RAID System is now ready for the installation of the Secure Path Software, as described in "Installing Secure Path Software" on page 43.

Installing Secure Path Software

3

This chapter describes how to install a new Secure Path software configuration. It contains the following information that is required for proper Secure Path installation and operation:

Note: Before attempting to install Secure Path software, read the Release Notes. The release notes may contain information not found in this installation and reference guide.

Installation prerequisites

Note: HSG80 controllers are not supported with 64-bit machines.

Before installing Secure Path v3.0C, verify the following requirements:

- The prerequisites listed in the *HP StorageWorks Secure Path v3.0C for Linux Release Notes* have been met.
- The procedures in "Hardware Setup" on page 29 have been performed.
- At least one unit is configured on the RAID storage system and is visible to the server from at least two paths. Ideally, and strongly recommended, the RAID storage systems should be configured with all the desired storagesets and units.
- For the EVA3000/EVA5000/HSG80—A supported QLA2300 driver must be installed. Ensure that you have installed the latest driver kit. Driver kits are available at http://h18006.www1.hp.com/products/storageworks/fca2214dc/index.html.
- For the MSA1000—A supported QLA2300 driver must be installed from the MSA1000 solution software CD and must recognize the LUNs on your MSA1000. For more MSA1000 information, access the following web site at: http://www.hp.com/go/msa1000.
- Ensure that you have successfully installed and configured the storage system hardware and software per the instructions that came with your storage system.

Installing Secure Path

Secure Path installation has been automated to use the Red Hat Package Management (RPM) utility installation.

If the installation process cannot complete for any reason, you will be instructed how to proceed manually. Every effort has been made to make your Secure Path software installation as simple and straightforward as possible, but given the large variations possible in system setup, manual intervention may be required.

Manually installing Secure Path

Secure Path v3.0C is installed based upon your operating system parameters. The following sections break down the installations in the following order:

1. Machine type: 32-bit or 64-bit
2. Full installation or Workgroup Edition
3. Red Hat or SUSE/UnitedLinux (64-bit only)

Install Secure Path software by performing the following procedures:

Caution: For each RAID system in a production environment that is being converted to Secure Path operation, make sure that all users have logged off the Linux servers and that **all** I/O to the RAID systems has ceased. Follow normal procedures to back up the storage systems before proceeding.

1. Insert the Secure Path v3.0C CD-ROM into the CD-ROM drive. A sample command follows:

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```

2. Change to the RPM directory. For example:

   ```
   # cd /mnt/cdrom/RPM
   ```

   You should be in the directory of the installation software RPM.

3. Choose one of the following installations based on your operating system parameters:
   - — To install Linux v3.0C or Linux v3.0C Workgroup Edition on 32-bit Red Hat operating systems, enter a command similar to the following:

     ```
     # rpm  -ivh Secure-Path-3.0C<Full or wkgrp>-
     <rev #>.noarch.rpm
     ```

     For example:

     ```
     # rpm  -ivh Secure-Path-3.0CFull-4.0.noarch.rpm
     ```

   - — To install the Linux v3.0C or Linux v3.0C Workgroup Edition on 64-bit Red Hat operating systems, enter a command similar to the following:

     ```
     # rpm -ivh Secure-Path-3.0C<Full or wkgrp>64-
     <rev #>.noarch.rpm
     ```

     For example:

     ```
     # rpm -ivh Secure-Path-3.0Cwkgrp64-3.0.noarch.rpm
     ```

   - — To install the Linux v3.0C or Linux v3.0C Workgroup Edition on a 64-bit SUSE/UnitedLinux installation, enter a command similar to the following:

     ```
     # rpm -ivh Secure-Path-3.0C<Full or wkgrp>UL64-
     <rev #>.noarch.rpm
     ```

     For example:

     ```
     # rpm -ivh Secure-Path-3.0CFullUL64-3.0.noarch.rpm
     ```

The RPM checks to ensure that the QLA2300 module is loaded.

If the QLA2300 module is not loaded, the following error message displays (Secure Path v3.0C for Linux is used as the example):

```
************************************************************

QLA2300 must be loaded to install this kit.

************************************************************

error: execution of %pre scriplet from Secure-Path -3.0CFull
-3.0 failed, exit status 255
```

The RPM ensures that the SMP or Enterprise (for Red Hat only) kernel is loaded. The following error message displays:

```
************************************************************

SMP or enterprise kernel must be loaded to install this kit

error: execution of %pre scriplet from Secure-Path -3.0CFull
Exiting . . .


************************************************************

error: execution of %pre scriplet from Secure-Path -3.0CFull

-3.0 failed, exit status 255

************************************************************
```

The RPM checks to ensure that the kernel is a supported version. If the kernel is not a supported version, the following error message displays:

```
************************************************************

You do not have a valid kernel version. Please see documentation
to see supported and allowed versions.

Exiting . . .

************************************************************
```

— If the kernel is supported, depending upon your operating system parameters, you may see one of the following errors:

Note: The following error messages apply to 32-bit systems only. If you try to install the 32-bit RPM on a SUSE/UnitedLinux 64-bit system, the following message displays:

```
************************************************************

This is IA64 based system. This installation only supports
32bit based systems.
Exiting.....

************************************************************
```

— For 32-bit SUSE/UnitedLinux with an unsupported errata version, but with a proper kernel version of 2.4.21-169-smp, the following error message displays:

```
************************************************************

You do not have a supported version of this
kernel(2.4.21-169-smp). If you want to install anyway,
please run the rpm with the --force command.(e.g. rpm -ivh
--force <package-name>)
Please see documentation for currently supported kernel
versions.

Exiting...

************************************************************
```

— For Red Hat 3.0 with a non-supported errata version, but with a proper kernel version of 2.4.21-9.ELsmp, the following error message displays:

```
************************************************************

You do not have a supported version of this kernel
(2.4.21-9.ELsmp) If you want to install anyway, please run
the rpm with the --force command.(e.g. rpm -ivh --force
<package-name>)
Please see documentation for currently supported kernel
versions.

Exiting...

************************************************************
```

— For Red Hat 2.1 with a non-supported errata version, but with a proper kernel version of 2.4.9-e.35smp, the following error message displays:

```
************************************************************

You do not have a supported version of this kernel
(2.4.9-e.35smp) If you want to install anyway, please run
the rpm with the --force command.(e.g. rpm -ivh --force
<package-name>)
Please see documentation for currently supported kernel
versions.

Exiting...

************************************************************
```

Note: The following error messages apply to 64-bit configurations only.

— If you do not have an IA64 base system, the following message displays:

```
************************************************************

This is an IA64 based system. This installation only
supports 32bit based systems.

Exiting...

************************************************************
```

— For Red Hat 3.0 IA64 with an unsupported errata version, but with a proper kernel version of 2.4.21-9.EL, the following error message displays:

```
************************************************************

You do not have a supported version of this
kernel(2.4.21-9.EL). If you want to install anyway, please
run the rpm with the --force command.(e.g. rpm -ivh --force
<package-name>)
Please see documentation for currently supported kernel
versions.

Exiting...

************************************************************
```

— For Red Hat 2.1 IA64 with an unsupported errata version, but with a proper kernel version of 2.4.18-e.41smp, the following error message displays:

```
************************************************************

You do not have a supported version of this
kernel(2.4.18-e.41smp). If you want to install anyway,
please run the rpm with the --force command.(e.g. rpm -ivh
--force <package-name>)
Please see documentation for currently supported kernel
versions.

Exiting...

************************************************************
```

— For the SUSE/UnitedLinux IA64 operating systems, if the kernel version is not valid the following message displays:

```
************************************************************

You do not have a supported version of this kernel
(2.4.21-112-itanium2-smp).
If you want to install anyway, please run the rpm with the
--force command. (e.g. rpm -ivh --force <package name>
Please see documentation for currently supported kernel
versions.

Exiting...

************************************************************
```

Automatically installing Secure Path

You can choose to automatically install the software as follows:

1. Insert the Secure Path v3.0C CD-ROM into the CD-ROM drive. A sample command follows:

   ```
   # mount /dev/cdrom /mnt/cdrom
   ```

2. Enter the following command:

   ```
   # ./install_SPlinux.sh
   ```

   The automatic installation scans the system to determine what OS and kernel is running and prompts you for verification. A sample of the installation script follows:

   ```
   ================================================================

   Welcome to the Secure Path Linux installer.
   ================================================================

   NOTES: Please make sure this script is being run on a supported
   linux kernel.  Please make sure the RPMs are resident in the RPM
   directory.

   Please wait while we check your system...
   ```

   — If you do not have a valid kernel, the following message displays.

   ```
   ****************************************************************

   The kernel on this system is not supported.  Please see
   documentation for supported kernel versions.
   Exiting...

   ****************************************************************
   ```

   — If you are not running the smp or enterprise kernel, the following message displays:

   ```
   ****************************************************************

   SMP or enterprise kernel must be loaded to install this kit.
   Exiting...

   ****************************************************************
   ```

   — If there is a valid errata/memory version, the kernel is valid. The following message displays:

   ```
   Your system is running <OS NAME>.  The kernel version is
   <Kernel Version>. This is a valid Kernel.

   Continuing with installation.
   ```

If you chose to continue, the installation is automatic from this point to completion.

— For 32-bit SUSE/ UnitedLinux operating systems, the system displays the following message if the errata version is not valid:

```
Your system is running UnitedLinux/SuSe 32bit. The kernel
version is 2.4.21-169-smp.
The system is not running the proper kernel
(2.4.21-141-smp).
The system is not running a proper kernel version.
Would you like to install anyway? [y/N]
```

If you choose N, the following message displays:

```
You have chosen not to continue. Exiting...
```

— For 64-bit SUSE/ UnitedLinux operating systems, the system displays the following message if the errata version is not valid:

```
Your system is running UnitedLinux/SuSe 64 bit. The kernel
version is 2.4.21-112-itanium2-smp.
The system is not running the proper kernel
(2.4.21-112-itanium2-smp).
The system is not running a proper kernel version.
Would you like to install anyway? [y/N]
```

If you choose N, the following message displays:

```
You have chosen not to continue. Exiting...
```

— The script displays the following for 32-Bit RHEL AS 2.1 if the errata version is not valid:

```
Your system is running RHEL AS 32bit. The kernel version is
2.4.9.
The system is not running the errata 35 kernel (2.4.9-e.35).
The system is not running a supported errata version.
Would you like to install anyway? [y/N]
```

If you choose N, the following message displays:

```
You have chosen not to continue.  Exiting...
```

— The script displays the following for 64-Bit RHEL AS 2.1 if the errata version is not valid:

```
Your system is running RHEL AS 64bit. The kernel version is
2.4.18.
The system is not running the errata 41 kernel
(2.4.18-e.41).
The system is not running a supported errata version.
Would you like to install anyways? [y/N]
```

If you choose N, the following message displays:

```
You have chosen not to continue. Exiting...
```

— The script displays the following for 32-Bit RHEL AS 3.0 if the errata version is not valid:

```
Your system is running RHEL AS 32bit. The kernel version is
2.4.21.
The system is not running the errata 9kernel (2.4.21-9.EL).
The system is not running a supported errata version.
Would you like to install anyway? [y/N]
```

If you choose N, the following message displays:

```
You have chosen not to continue. Exiting...
```

— The script displays the following for 64-Bit RHEL AS 3.0 if the errata version is not valid:

```
Your system is running RHEL AS 64bit. The kernel version is
2.4.21.
The system is not running the errata 41 kernel
(2.4.21-9.EL).
The system is not running a supported errata version.
Would you like to install anyways? [y/N]
```

If you choose N, the following message displays:

```
You have chosen not to continue. Exiting...
```

If the system has a valid kernel version or if you answer **yes** to any of the above questions, the appropriate RPM is installed. An `rpm -ivh` or an `rpm -ivh --force` is issued by the installation script.

An installation log file is created as a result of running the above command and contains any errors encountered. If the directory `/var/log/h` exists on your system, the installation log messages are placed in `/var/log/sp_log`. If the `/var/log` directory does not exist on your system, a log file named `sp_install_results.log` is created in the `/root` directory.

Check the log file for any errors. If there were no errors, reboot your system and go to "Using Secure Path persistence software" on page 55 for more information on `sps`, the LUN persistence program.

If there were errors during the installation of Secure Path software, you must fix the problems before proceeding. Refer to "Fibre Channel Device Software" on page 113 for a complete explanation of possible problem causes and recovery actions.

Configuration files added by Secure Path

Table 4 lists the files added as part of the Secure Path v3.0C installation.

Table 4: Configuration files

File name	Description
hsx.conf	Used by *spagent* to make preferred path settings persistence across reboots. Whenever you modify the preferred path setting, *spagent* modifies *hsx.conf*. After rebooting, *spagent* reads the file and sends an appropriate IOCTL call to mark the path to *Preferred*.
swsp.conf	Used by *spagent* to make various settings persistence across reboots. It stores global as well as per storage system Path Verification, Load Balance and Auto-Restore settings.
notify.ini	Contains the e-mail address of the user and the level of notification. The *spmgr* utility and *spagent* agent sends the event notification to the user based upon the entry in this file.
spmgr_alias	Contains the alias name used for various Secure Path entities. The *spagent* daemon uses this file to decode the alias name into the original name of the entity.
spmgr_stop_list	Contains a list of reserved key word. The *spmgr* utility uses this file to restrict the use of reserved key words as an alias.
sppf	ASCII data for Secure Path persistence. This file contains LUN IDs, device special files, and symbolic link information.
clients	Stores spmgr password information.

Using Secure Path persistence software

After you have rebooted the system, you can find symbolic links to real devices in the `/dev/spdev` directory. These links were created by the Secure Path Persistence Software `(sps)`, a LUN persistence program written to work with Secure Path. All disk operations should be done via these links and not the real device name. For a detailed explanation of `sps` and LUN persistence, refer to "Fibre Channel Device Software" on page 113.

Managing Secure Path

4

This chapter describes the user interface for the Secure Path v3.0C Management utility `spmgr`. It includes the following topics:

Note: Examples are based on the MSA1000 controller, but all actions are identical for the HSG80 and HSV110/HSV100 controllers.

Secure Path Manager overview

The Secure Path Manager (`spmgr`) utility lets you monitor and manage devices, storage systems, and paths to units that are in the Secure Path configuration. It also lets you modify the configuration to repair, replace, or reconfigure. The `spmgr` utility relies on `spagent` to handle calls to the driver (`swsp`).

Adding or deleting LUNs

Secure Path v3.0C for Linux does not support adding and deleting LUNs dynamically. However, you can manually add and delete LUNs by performing the following steps:

1. Shut down your server.
2. Add or delete LUNs from your controller. Refer to your storage system documentation for more information on adding or deleting LUNs from your controllers.
3. Boot your server.

Note: When you remove LUNs that will not be returned from Secure Path control, you should also remove them from the Persistence database. Refer to "Fibre Channel Device Software" on page 113 for more information on the Persistence database.

Spmgr commands

Table 5 lists the `spmgr` command options. Their format and usage are presented and described in the sections following the tables.

Table 5: *Spmgr* commands

Command	Options / Arguments	Description
spmgr alias	alias_name old_name no argument	Assigns an alias to an object.
spmgr display	-a[v] [adapter] -c[v] [controller_ser_num] -d[v] [device] -p path-Instance -r[v] [WWNN] no argument	Displays information about configured Secure Path devices, controllers, adapters, paths, and arrays.
spmgr log	-c 0, 1...3 -l 0, 1...3 -n 0, 3 no argument	Displays and sets logging to the console, system log file, and e-mail notification.
spmgr notify	add severity_level email_address delete email_address no argument	Manages and displays e-mail address and event logging severity to each e-mail recipient.
spmgr passwd	passwd <new password>	Changes default password to a unique password.
spmgr prefer	path_instance	Assigns a preferred attribute to a path.
spmgr quiesce	-a adapter -c controller_ser_num -p path_instance	Moves I/O to an alternative object and temporarily removes selected object from use.
spmgr restart	-a adapter -c controller_ser_num -p path_instance all	Returns a previously quiesced object to an active or available state.

Table 5: *Spmgr* commands (Continued)

Command	Options / Arguments	Description
spmgr restore	-d device -r WWNN all	Restores one or more devices to their preferred I/O path.
spmgr select	-a adapter [-d device] -c controller_ser_num [-d device] -p path_instance	Selects a path for I/O.
spmgr set	-a on | off [WWNN] -b on | off [WWNN] -f interval -p on | off [WWNN]	Enables or disables special driver functionality.
spmgr unalias	alias_name old_name	Deletes an alias.
spmgr unprefer	path_instance	Removes a preferred path attribute.

Note: Commands typed without an argument respond with *usage* if the command is a configuration altering command. The commands-`alias, display, log`, and `notify`-respond with current command or configuration information.

Spmgr common terms

Table 6 describes the common `spmgr` terms. For a more complete list of Secure Path glossary terms, refer to page 119 in this book.

Table 6: Spmgr common terms

Term	Definition
Device	The standard representation for a device or device link on a server, for example, `spa`
Logical Unit	A device that is managed by Secure Path and identified by its 32-digit World Wide LUN Identifier (WWLUNID).
Adapter	The operating system ID of the HBA. For example: `2300-0, 2300-1`
Storage System Array WWNN	A storage system is identified by its 16-digit World Wide Node Name (WWNN).
Controller serial number	The controller is identified by a unique serial number. The serial number of the HSG80 is a 10-character alphanumeric string. For the HSV110, HSV100, and MSA1000, the serial number is a 14-character alphanumeric string.

Displaying configuration information

Controller states

Table 7 lists the possible controller states and their descriptions.

Table 7: Controller states

Controller states	Description
Failed	This state may mean a failed or offline condition because the server cannot communicate with the other controller at this time.
Operational	The controller is available with a good status.
Unknown	The server cannot communicate with this controller.

Path states and attribute

Table 8 describes the path states reported by the Secure Path driver.

Table 8: Path states and attribute

Path states/attribute	Description
Active	This state indicates that the path is currently used for the I/O stream.
Available	This state indicates that the path is available on the active controller for the I/O stream.
Failed	This state indicates that the path is currently unusable for the I/O stream.
Quiesced	This state indicates that the path may be valid, but has been made unavailable for I/O.
Standby	This state indicates that the path is valid on the standby controller.
Preferred	This attribute indicates that the path is preferred for the I/O stream, across reboots.

Device states

Table 9 lists and describes device states.

Table 9: Device states and description

Device States	Description
Critical	Only one path remains available to the storage unit.
Degraded	At least one or more paths are failed to the storage unit.
Operational	All paths are available to the storage unit.
Unknown	Unable to communicate with the unit. This may indicate no available path or a failed device.
Failed	Paths are available but an inquiry to the device returns a not-ready state even after retries.

Display header information

The display information always has two standard lines of information at the start of the display:

Line 1: Server: Server Name Report Created: Date and Time

Line 2: Command: Command string

Display differences between HSG80, HSV110/HSV100, and MSA1000 controllers

All general examples in this document use the MSA1000 serialization format and actual MSA1000 examples. The HSG80, HSV110/HSV100, and MSA1000 present objects to Secure Path in identical ways. There is no difference in the way you manage settings, paths, and devices using the `spmgr` management utility.

For the HSG80 and HSV110/HSV100, there are two differences in serialization of array objects that allow you to quickly determine which type of array is being displayed. The following examples list the differences:

HSG80

```
World Wide  Node Name (WWNN): 5000-1FE1-0016-68C0

World Wide LUN ID(WWLUNID):
6000-1FE1-0016-68C0-0009-2040-0315-002E

Controller Serial Number: ZG20400315
```

HSV110/HSV100

```
World Wide  Node Name (WWNN): 5000-1FE1-0015-0AE0

World Wide LUN ID(WWLUNID):
6005-08B4-0001-40BF-0000-A000-1234-0000

Controller Serial Number: P4889B29LC01J
```

In the HSG80 and HSV110/HSV100 examples, the location of the sequence `1234` in the WWLUNID examples is unique to each LUN and is in a different position in the array types.

For the HSV110, HSV100, and MSA1000, the controller serial number is a 14-position alphanumeric string and for the HSG80, controller serial numbers are a 10-position alphanumeric string.

MSA1000:

```
World Wide  Node Name (WWNN): 5008-05F3-0000-6FD0

World Wide LUN ID(WWLUNID):
6008-05F3-0000-6FD0-0000-0000-3F30-0043

Controller Serial Number: P56350A9IMN19M
```

The display command

This section describes the `spmgr display` commands and associated switch parameters. Each switch results in a different type of display.

Note: The verbose flag may only be used with some, but not all, cases of the command.

Syntax:

```
# spmgr display -a[v] [adapter]
          -c[v] [controller_ser_num]
          -d[v] [device]
          -p path_instance
          -r[v] [WWNN]
          (no argument)
```

For each of these command switches, this section presents:

- Description
- Syntax

spmgr display

When you enter `spmgr display`, all information for the entire configuration is displayed. The amount of information displayed depends on the number of HBAs, storage systems, and paths to a unit on each storage system.

The full display derives from the component portions described in this section. You can limit the amount of data displayed by combining the `spmgr display` command with one of the described switches.

Example:

```
# spmgr display
Server:  sensodyne    Report Created: Fri, Jul 12 10:50:30 2002
Command: spmgr display
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5008-05F3-0000-6FD0
Load Balance: Off  Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: 2300-1  2300-2
Controller:  P56350A9IMN19M, Operational
             P56350A9IMN0XI, Operational
Devices:  spf  spg  sph  spi
TGT/LUN   Device          WWLUN_ID                      #_Paths
  0/  0    spf       008-05F3-0000-6FD0-A977-751F-E54F-0022   2
  Controller  Path_Instance       HBA    Preferred?  Path_Status
  P56350A9IMN19M                          no
       hsx_mod-1-0-0-1           2300-1   no          Standby
  Controller  Path_Instance       HBA   Preferred?  Path_Status
      P56350A9IMN0XI                      YES
       hsx_mod-2-0-0-1           2300-2   no          Active
TGT/LUN   Device          WWLUN_ID                     #_Paths
  0/  1    spg       6008-05F3-0000-6FD0-A727-6527-BE0B-0027   2
  Controller  Path_Instance       HBA   Preferred?  Path_Status
```

```
    P56350A9IMN19M                          no
       hsx_mod-1-0-0-2            2300-1    no        Standby
  Controller  Path_Instance       HBA    Preferred? Path_Status
    P56350A9IMN0XI                         YES
       hsx_mod-2-0-0-2            2300-2    no         Active
TGT/LUN   Device          WWLUN_ID                  #_Paths
  0/  2    sph       6008-05F3-0000-6FD0-A057-552D-DBB4-002B   2
Controller   Path_Instance        HBA    Preferred? Path_Status
   P56350A9IMN19M                          no
      hsx_mod-1-0-0-3              2300-1  no          Standby
Controller   Path_Instance       HBA   Preferred?  Path_Status
   P56350A9IMN0XI                        YES
      hsx_mod-2-0-0-3            2300-2   no            Active
TGT/LUN   Device          WWLUN_ID                  #_Paths
  0/  3    spi       6008-05F3-0000-6FD0-AA77-454F-E3C4-0023   2
Controller   Path_Instance       HBA  Preferred?   Path_Status
    P56350A9IMN19M                         no
     hsx_mod-1-0-0-4           2300-1    no            Standby
Controller   Path_Instance       HBA  Preferred?   Path_Status
    P56350A9IMN0XI                        YES
    hsx_mod-2-0-0-4          2300-2      no            Active
```

spmgr display -a[v] [HBA]

The `-a` switch lists HBA (host bus adapter) related information. If a parameter is supplied, it must be the *adapter instance number*.

Syntax:

```
# spmgr display -a
          -av
          -a HBA
          -av HBA
```

When the `-a` switch is used without a parameter, the display contains a complete list of all HBAs in the Secure Path configuration from the server where the command is entered.

Example:

```
# spmgr display -a
Server:  sensodyne  Report Created: Fri, Jul 12 10:57:12 2002
Command: spmgr display -a
Adapters in the Secure Path Configuration
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
2300-1, 2300-2
```

When the -av switch is used, the display contains a list of all adapters in the Secure Path configuration.

Example:

```
# spmgr display -av
Server:lotus       Report Created: Tue, Oct 01 09:52:38 2002
Command: spmgr display -av
Adapter                                        Driver Version
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
2300-1                                      6.04.00
2300-2                                      6.04.00
```

When invoked with the -a or -av switch and HBA, the display shows the Linux path attached to the HBA, as shown in the following example:

Example:

```
# spmgr display -a 2300
Server:  swsp91 Report Created: Thu, Oct 02 17:04:45 2003
Command: spmgr display -a 2300-0
Adapter              Driver Version
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
2300-0               v.6.04.00
```

Example:

```
# spmgr display -av 2300-0
  Server:  swsp91    Report Created: Thu, Oct 02 15:58:32 2002
  Command: spmgr display -av 2300-0
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  Adapter: 2300-0       Version: v.6.04.00
```

spmgr display -c[v] [controller_serial_number]

The `-c` switch displays controller related information. If a parameter is supplied, it must be a *`controller_serial_number`*. The command has four possible forms:

Syntax:

```
# spmgr display     -c
                    -cv
                    -c controller_serial_number
                    -cv controller_serial_number
```

Example:

```
# spmgr display -c
Server:  sensodyne    Report Created: Fri, Jul 12 10:58:44 2002
Command: spmgr display -c
Current Controller List
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
P56350A9IMN19M, P56350A9IMN0XI
Example:
# spmgr display -cv
Server:  lotus  Report Created: Tue, Oct 01 09:54:18 2002
Command: spmgr display -cv
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  Controller: P56350A9IMN19M  Status: Operational
  Vendor: HP
  WWNN: 5008-05F3-0000-6FD0
  WWPN1: 50001FE1500038A8
  HBAs:  2300-1, 2300-2
```

```
Controller: P56350A9IMN0XI  Status: Operational
  Vendor: HP
  WWNN: 5008-05F3-0000-6FD0
  WWPN1: 50001FE15000388C
  HBAs:  2300-1, 2300-2
```

Example:

```
# spmgr display -c controller_serial_number
Server:  sensodyne    Report Created: Fri, Jul 12 11:05:30 2002
 Command: spmgr display -c P56350A9IMN0XI
 = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
 Controller: P56350A9IMN0XI  Status: Operational
 Vendor: HP
 WWNN: 5008-05F3-0000-6FD0
 HBAs: 2300-2
```

Example:

```
# spmgr display -cv P56350A9IMN19M
Server:  sensodyne    Report Created: Mon, Jul 15 08:43:25 2002
Command: spmgr display -cv P56350A9IMN19M
   = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Controller: P56350A9IMN19M  Status: Operational
Vendor: HP
WWNN: 5008-05F3-0000-6FD0
HBAs: 2300-1
Item  Device       Controller     HBA        Instance
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  0   spf       P56350A9IMN19M   2300-1      hsx_mod-1-0-0-1
      WWPN: 5008-05F3-0000-6FD1  Path State: Standby
  1   spg       P56350A9IMN19M   2300-1      hsx_mod-1-0-0-2
      WWPN: 5008-05F3-0000-6FD2  Path State: Standby
```

spmgr display –d[v] [device]

The -d switch displays device related information. If a parameter is supplied, it must be a *device*.

```
Syntax:
# spmgr display     -d
                    -dv
                    -d[device]
                    -dv[device]
```

Example

```
# spmgr display -d
Server:  sensodyne    Report Created: Fri, Jul 12 11:06:16 2002
Command: spmgr display -d
Devices by Storage System
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5008-05F3-0000-6FD0
Devices:  spf  spg  sph  spi  spj  spk  spl  spm  spn  spo  spp
spq  spr sps  spt  spu  spv  spw  spx  spy  spz  spaa  spab  spac
spad  spae  spaf spag  spah  spai  spaj  spak
```

Example:

```
# spmgr display -dv
Server:  sensodyne    Report Created: Fri, Jul 12 11:07:01 2002
Command: spmgr display -dv
Device:       spf
Status:        Operational  [2 paths (1/0/1)]
Storage:      5008-05F3-0000-6FD0
LUNID:      6008-05F3-0000-6FD0-A977-751F-E54F-0022
Preferred Controller: P56350A9IMN0XI
HBAs:  2300-1 2300-2
Device:       spg
Status:        Operational  [2 paths (1/0/1)]
Storage:      5008-05F3-0000-6FD0
```

Note: Secure Path displays path states using the following convention:
[total number of paths (active/failed/standby)].
Actual numerical equivalents replace the text.
For example, the following attributes are displayed as [10 paths (8/0/2)]:
Total paths = 10, Active = 8, Failed = 0, Standby = 2

Example:

```
# spmgr display -d spf
  Server:  sensodyne Report Created: Mon, Jul 15 08:46:34 2002
  Command: spmgr display -d spf
  Device:       spf
  Status:       Operational  [2 paths (1/0/1)]
  Storage:      5008-05F3-0000-6FD0
  LUNID:        6008-05F3-0000-6FD0-A977-751F-E54F-0022
  Preferred Controller: P56350A9IMN0XI
  HBAs:  2300-1 2300-2
```

Example

```
# spmgr display -dv spa
Server:  swsp58.mro.cpqcorp.net Report Created: Thu, Oct 02
16:00:28 2003
  Command: spmgr display -dv spa
  Device:       spa
  Status:       Operational  [4 paths (1/0/2)]
  Storage:      5000-1FE1-0015-A370
  LUNID:        6000-1FE1-0015-A370-0009-1050-6937-002E
  Preferred Controller: None
```

```
  HBAs:  2300-2 2300-4
Item  Device       Controller HBA         Instance
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  0     spa      ZG10506937 2300-2      hsx_mod-2-0-0-1
        WWPN: 50001FE10015A374     Path State: Active
  1     spa      ZG10707577 2300-2      hsx_mod-2-0-1-1
        WWPN: 50001FE10015A372     Path State: Standby
  2     spa      ZG10707577 2300-4       hsx_mod-4-0-0-1
        WWPN: 50001FE10015A374     Path State: Standby
  3     spa      ZG10506937 2300-4       hsx_mod-4-0-1-1
        WWPN: 50001FE10015A372     Path State: Available
```

spmgr display –p path_instance

The `-p` *`path_instance`* displays path instance information.

Example:

```
# spmgr display -p hsx_mod-1-0-0-32
Server:  sensodyne    Report Created: Fri, Jul 12 11:18:39 2002
Command: spmgr display -p hsx_mod-1-0-0-32
Path:          hsx_mod-1-0-0-32            Status:   Standby
Controller: P56350A9IMN19M          Status:  Operational
Device:     spak                    Status:  Operational
Adapter:    2300-1
```

spmgr display –r[v] [WWNN]

The `-r` switch displays storage system information. If a parameter is supplied, it must be a *`WWNN`*. The command has the following possible forms:

Syntax:

```
# spmgr display  -r
          -rv
          -r WWNN
          -rv WWNN
```

Example:

```
# spmgr display -r
Server:  sensodyne    Report Created: Fri, Jul 12 11:20:10 2002
Command: spmgr display -r
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5008-05F3-0000-6FD0
```

Example:

```
# spmgr display -rv
Server:  sensodyne    Report Created: Fri, Jul 12 11:21:13 2002
Command: spmgr display -rv
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5008-05F3-0000-6FD0
Load Balance: Off   Auto-restore: Off
Path Verify:    On    Verify Interval: 30
HBAs: 2300-1  2300-2
Controller:  P56350A9IMN19M, Operational
             P56350A9IMN0XI,  Operational
 Devices:  spf  spg  sph  spi  spj  spk  spl  spm  spn  spo  spp
spq spr  sps  spt  spu  spv  spw  spx  spy  spz  spaa  spab spac
spad  spae  spaf  spag  spah  spai  spaj  spak
```

Example:

```
# spmgr display -r 5008-05F3-0000-6FD0
Server:  sensodyne    Report Created: Mon, Jul 15 08:47:42 2002
Command: spmgr display -r 5008-05F3-0000-6FD0
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5008-05F3-0000-6FD0
Load Balance: Off  Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: 2300-1  2300-2
Controller: P56350A9IMN19M, Operational
            P56350A9IMN0XI, Operational
Devices:  spf  spg  sph  spi  spj  spk  spl  spm  spn  spo  spp
spq spr  sps  spt  spu  spv  spw  spx  spy  spz  spaa  spab spac
spad  spae  spaf  spag  spah  spai  spaj  spak
```

Example:

```
# spmgr display -rv WWNN
Server:  sensodyne    Report Created: Fri, Jul 12 11:22:00 2002
Command: spmgr display -rv 5008-05F3-0000-6FD0
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5008-05F3-0000-6FD0
Load Balance: Off  Auto-restore: Off
Path Verify:   On    Verify Interval: 30
HBAs: 2300-1  2300-2
Controller:  P56350A9IMN19M, Operational
             P56350A9IMN0XI,  Operational
Devices:  spf  spg  sph
TGT/LUN   Device       WWLUN_ID                          #_Paths
0/  0      spf       6008-05F3-0000-6FD0-A977-751F-E54F-0022   2
Controller  Path_Instance      HBA   Preferred?      Path_Status
P56350A9IMN19M                          no
        hsx_mod-1-0-0-1       2300-1    no             Standby
Controller  Path_Instance      HBA   Preferred       Path_Status
P56350A9IMN0XI                          YES
        hsx_mod-2-0-0-1       2300-2    no             Active
TGT/LUN   Device       WWLUN_ID
                           #_Paths
  0/  1    spg       6008-05F3-0000-6FD0-A727-6527-BE0B-0027   2
Controller  Path_Instance      HBA   Preferred?      Path_Status
P56350A9IMN19M                          no
        hsx_mod-1-0-0-2       2300-1    no           Standby
Controller  Path_Instance      HBA   Preferred       Path_Status
P56350A9IMN0XI                          YES
        hsx_mod-2-0-0-2       2300-2    no           Active
TGT/LUN   Device     WWLUN_ID                             #_Paths
  0/  2    sph      6008-05F3-0000-6FD0-A057-552D-DBB4-002B    2
Controller  Path_Instance      HBA   Preferred?      Path_Status
```

```
P56350A9IMN19M                          no
       hsx_mod-1-0-0-3        2300-1    no           Standby
Controller  Path_Instance      HBA    Preferred?    Path_Status
P56350A9IMN0XI                         YES
    hsx_mod-2-0-0-3         2300-2    no              Active
```

The alias and unalias commands

Secure Path supports the use of aliases. Aliases substitute default names for custom names.

Example:

The World Wide Node Name (WWNN) of a storage system is `5000-1FE1-0005-3480.` You can assign the alias `Fire` to replace the longer, less easy-to-remember WWNN `5000-1FE1-0005-3480.`

When an alias is used in an `spmgr` display, it is shown in parenthesis after the term that it substitutes for.

Example:

```
Storage: 5000-1FE1- 0005-3480 (fire)
```

The alias is `fire.`

Alias commands:

- Define an alias and store it for future use
- Remove an alias from the alias table
- Display the alias table

spmgr alias alias_name old_name

To add an alias to the alias table, use the following `alias` command.

Syntax:

```
# spmgr alias alias_name old_name
```

The following example creates the alias `Birdtop` for the controller serial number `P56350A91MN19M`.

```
# spmgr alias Birdtop P56350A91MN19M
```

spmgr unalias

To remove an alias from the alias table, invoke the `spmgr unalias` command and enter either the *`alias_name`* or the *`old_name`*.

Syntax:

```
# spmgr unalias  old_name
                 alias_name
```

In the following example, the alias, `Birdtop`, is removed from the alias table.

```
# spmgr unalias Birdtop
```

spmgr alias

Use the `spmgr alias` command to display the alias table.

Syntax:

```
# spmgr alias
```

Example:

```
# spmgr alias
Server:  Pluto Report Created: Wed, Aug 15 15:42:37 2001
Alias:old_string
= = = = = = = = = = = = = =
bob:5000-1fe1-0000-1231
jim:5000-1fe1-0000-1233
fredt:ZG111298235442
fredb:ZG238817633215
= = = = = = = = = =  = =  = =
```

Note:

- When the `spmgr display` command is invoked, the screen output uses both the alias, if any, and the standard storage system WWNN or controller serial number. The alias will be enclosed in parentheses (alias_name).
- For a command set that requires a parameter, it is assumed that the parameter or its alias may be input. Commands cannot be aliased.

Setting storage system parameters

The Secure Path v3.0C driver has options you can enable or disable on a storage system or global basis. These options may be turned off and on dynamically. These changes occur within 45 seconds.

- The `spmgr set` command lets you enable storage system specific settings for the Secure Path driver.
  - **Load Balancing**– v3.0C of Secure Path implements a round-robin usage of all available paths to a unit for its I/O. The default for Load Balancing is disabled.
  - **Path Verification**–The driver checks the state of all possible paths to all units at a settable period or frequency. The default for Path Verification is enabled with a period of 30 seconds.
  - **Auto-Restore**–The `Auto-Restore` command enables the driver to automatically restore paths to their preferred path after a failure and subsequent reinstatement of that path. The default for `Auto-Restore` is **disabled**.
- The `spmgr log` command lets you enable logging from the Secure Path driver to the syslog, console, and e-mail notification.
- The `spmgr notify` command lets you manage the distribution of the three classes of event reports (critical, warning, and informational) via an e-mail address list.

The set command

Syntax:

```
# spmgr set -a (on | off) [WWNN]
            -b (on | off) [WWNN]
            -p (on | off) [WWNN]
            -f verify_period
```

spmgr set -a on | off [WWNN]

This command enables or disables the Auto-Restore feature of the driver. When Auto-Restore is enabled, it directs the driver to monitor the state of the paths. If the preferred path should fail and then later return to service, the driver automatically reroutes all I/O to the restored path. When Auto-Restore is disabled, there is no Auto-Restore by the Secure Path driver. The I/O continues along the current paths until another event changes the active path. The default is disabled.

spmgr set -b on | off [WWNN]

This command enables or disables the Load Balancing option of the driver. When Load Balancing is enabled, I/O is sent to the unit along all available paths. When Load Balancing is disabled, the I/O is sent along the Preferred Path (if one is selected) or uses the first available path for I/O. The default is disabled.

spmgr set -p on | off [WWNN]

This command enables or disables the path verification of the driver. When enabled, this command verifies the state of all possible paths to all units. On large configurations with active I/O to many units, this command may reduce performance. The default is enabled.

spmgr set -f (1…65535 seconds)

This command sets the path verification interval. This interval can be set between 1 to 65535 seconds. The use of the `-f` switch does not change the current state of the path verification. It will only change the value for the interval. Therefore, if path verification is disabled, it remains disabled with the new interval. The default is 30 seconds.

The log command

Syntax:

```
# spmgr log -l (level  0, 1,2,3)
            -c (level  0, 1,2,3)
            -n (level  0, 3)
```

The numerical level indicates the message severity. The levels of severity are:

1: Critical, 2: Warning, 3: Informational

When you select a numerical level, messages of that severity and higher are delivered to the appropriate output.

- If 3 is selected, then 3, 2, 1 are logged.
- If 2 is selected, then 2, 1 are logged.
- If 1 is selected, then 1 is logged.
- If 0 is selected, then logging is disabled for that item.

spmgr log -l [0, 1..3]

This command sets the level of logging to the syslog of the server. When you select level 1…3, the messages of that severity and higher are written to the `syslog` file. The default is 2.

spmgr log -c [0,1..3]

This command sets the level of logging to the console. When you select level 1..3, the messages of that severity and higher are displayed on the console. The default is 1.

spmgr log -n [0, 3]

This command enables or disables logging to the notify function. This option has two values, 0 and 3. The default is 3. Level 0 is provided for disabling all notification messages.

```
# spmgr log
Server:  sensodyne    Report Created: Fri, Jul 12 11:29:03 2002
Command: spmgr log
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Current Log Options
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Syslog,          enabled,          level 2
Console,         enabled,          level 1
Notify,          enabled,          level 3
```

The notify command

The notify command lets you manage the distribution of the three classes of event reports: critical, warning, and informational. In Secure Path v3.0C, notification occurs through e-mail messages.

Syntax:

```
#spmgr  notify add
                delete
                (no argument)
```

Messages from the Secure Path drivers are one of three severity levels:

- Critical messages are severity level 1.
- Warning messages are severity level 2.
- Informational messages are severity level 3.

Notify sends event notices to users from the highest to the lowest level of the severity marking as follows:

- A user with severity level 3 receives level 3, 2, and 1 severity messages.
- A user with severity level 2 receives level 2 and 1 severity messages.
- A user with severity level 1 receives severity level 1 messages only.

spmgr notify add

This command adds an e-mail address to the notification list.

Syntax:

```
# spmgr notify add severity_level  email_address
```

Example:

```
# spmgr notify add 3 john.doe@oscar.edu.it
```

Severity_level is 3 and the email_address is john.doe@oscar.edu.it.

Note: A user is defined by a unique email_address. A user with more than one email_address may have multiple records, one for each unique address.

---

spmgr notify delete

This command deletes an e-mail address from the notification list.

Syntax:

```
# spmgr notify delete email_address
```

Example:

```
# spmgr delete julie.smith@hollywood.edu.
```

The deleted email_address is julie.smith@hollywood.edu.

spmgr notify

This command displays the list of users to be notified that have been saved in configuration files.

Example:

```
# spmgr notify
Server:  sensodyne    Report Created: Fri, Jul 12 11:28:09 2002
Command: spmgr notify
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Severity        Mode          email_address
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
      3          M              root
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

Path management

Secure Path v3.0C supports up to 32 paths to a unit on a storage system. The `spmgr` utility lets you monitor and manage these paths.

The path management tasks include:

- Selecting paths
- Setting preferred and unpreferred paths
- Restoring preferred paths
- Quiescing and restarting objects and paths

The select command

A path is a combination of all the components from server to the unit on the storage system. When you describe the entire path you must identify the HBA and the controller port.

Selecting paths means to identify a path to be used for I/O. Path information, including *selected* paths, can be viewed with one or more options of the `spmgr display` command.

- When paths are selected for I/O and are intended to remain selected during a server reboot or power cycle, they are referred to as *preferred paths*.
- If paths are selected for the duration of the server's current processing time, they are referred to as *selected paths* and are not preserved during a reboot or power cycle of the server.

Syntax:

```
spmgr select  -a HBA [-d device]
              -c controller_ser_num [-d device]
              -p path_instance
```

spmgr select -a HBA

This command selects the path with the indicated HBA conditions and makes that path Active.

Example:

```
# spmgr select -a 2300-1
```

Result: The Secure Path driver selects all paths from 2300-1 to all units on all storage systems and marks them *selected*.

spmgr select -a HBA –d device

This command selects the path with the indicated HBA and device and makes that path *Active*.

Example:

```
# spmgr select –a 2300-1 –d spa
```

Result: The Secure Path driver selects one path from 2300-1 to unit `spa` and marks it *selected*.

spmgr select -c controller_serial_number

This command selects the path with the indicated controller serial number and makes that path *Active*. For example, if there are three HBAs with paths through one controller, the Secure Path driver marks one path for each device from one HBA, not necessarily the same HBA. The result is to have identified selected paths for multiple units with this command.

Example:

```
# spmgr select –c P56350A91MN19M
```

Result: The Secure Path driver selects each path through the controller, P56350A91MN19M, to each unit for I/O.

spmgr select -c controller_serial_number -d device

This command selects the path with the indicated controller and device and makes that path *Active.* This command selects one controller. Therefore, the driver is able to mark one path for each device on that controller as *selected.* This command indicates which controller to begin selecting and which unit to end marking. If you have three HBAs with paths through that controller, the Secure Path driver will mark one path for the device from one HBA. The overall result is to have identified selected paths for a single unit with this command.

Example:

```
# spmgr select –c P56350A91MN19M –d spa
```

Result: The Secure Path driver selects each path through the controller, P56350A91MN19M, to unit spa as the selected path for I/O.

spmgr select -p path_instance

This command selects the indicated path and makes that path *Active*. This parameter, `path_instance,` satisfies the path equation because it contains the necessary components of HBA, controller port, and device. Therefore, no other switches or parameters are required to identify the path.

Example:

```
# spmgr select -p hsx-mod-1-0-0-2
```

Result: The Secure Path driver selects path `hsx-mod-1-0-0-2` for I/O.

The prefer and unprefer commands

On an array, each LUN may be assigned to a particular controller and be available for selection at startup.

Because Secure Path can have more than one path to each controller, you can further specify a *preferred path*. To differentiate between the controller unit attribute of *Preferred_path* and the Secure Path *preferred path,* this document refers to the controller-based Preferred_path attribute as the *preferred controller.*

The preferred path assignment lets you control setting static Load Balancing because the path chosen determines which adapter and controller port are designated as the default path at system startup. One preferred path can be assigned to each controller for each LUN.

For the Preferred Path feature to work, the preferred path attribute on Secure Path must be set. For the HSG80, HSV110 and HSV100, the preferred controller can be set. For the MSA1000, the preferred controller is set up by default.

At any time you can select a different path to be used for I/O. The selected path is not preserved for a server power cycle or operating system restart. To preserve an active path through power cycles and restarts, identify it as a *preferred path*. Preferred path identifications are marked by the Secure Path driver in the running system, and the identifications are stored in the configuration files for that driver. Therefore, the path may be maintained permanently until removed or another preferred path is selected.

To support adding and removing preferred paths, `spmgr` provides two commands, `spmgr prefer` and `spmgr unprefer`.These two commands each require a single parameter: the `path_instance`.

spmgr prefer path_instance

This command instructs the Secure Path driver to mark a designated path as *Preferred*. If load balance is disabled, this path becomes the active I/O path. Additionally, `spmgr` adds this path_instance to the Secure Path driver's configuration file and upon reboot of the server, the preferred paths will be restored.

Syntax:

```
# spmgr prefer path_instance
```

Example:

```
# spmgr prefer hsx_mod-1-0-0-2
```

This command requires that the *`path_instance`* be supplied on the command line. The *`path_instance`* is provided in the `spmgr display` listings.

spmgr unprefer path_instance

This command instructs the Secure Path driver to unmark the path as a preferred path. Additionally, the configuration file for the Secure Path driver is modified by removing the preferred path markings.

Syntax:

```
# spmgr unprefer path_instance
```

Example:

```
# spmgr unprefer hsx_mod-1-0-0-2
```

Impact of Load Balancing and active Paths

For storage systems, *preferred* path and *selected path* are meaningless designations when you have enabled Load Balancing. Load Balancing directs I/O to all *available* paths. In other words, Load Balancing is a higher priority than *Preferred* or *selected* paths.

When Load Balancing is enabled, the Secure Path driver attempts to use all the *available* paths to a LUN in a round-robin fashion.

If Load Balancing is enabled and you set the path as *Preferred*, the system performs the following actions:

- The driver marks the path as *Preferred,* but the path will not be used as *Preferred* until the Load Balancing is turned off.

- The configuration file for paths have this path marked as *Preferred*. Upon reboot, this path will be marked as *Preferred* and deployed as *Preferred* if and when Load Balancing is disabled.

If Load Balancing is enabled and you select a path, the system performs the following actions:

- If the path is on the standby controller, I/O moves to the standby controller and the selected path is one of the *Active* paths.
- If the path is on the active controller, the path continues to be used as one of the set of *Active* paths.

Note: This selection and marking is not preserved across reboots or power cycling.

The restore command

Once a path has failed or has been taken off line by one or more events, the `spmgr restore` command lets you restore one or more LUNS to their preferred I/O path. This command lets you manually restore all or part of a configuration when the Auto-Restore feature has been disabled.

A path to a device consists of an adapter (HBA) and a port on a controller (WWNN). A unit on a storage system may be seen through several paths, for example, more than one HBA and controller. The default for `spmgr restore` is to return all LUNs to their preferred path. It will transition all LUNs to their preferred controller and their adapter if one has been specified and if Load Balancing is disabled.

By using one or more of the switches for this command, you have control of restoring preferred paths using the following restore options:

- If there is a preferred controller and:
  - A preferred path on each controller, then the preferred path on the preferred controller becomes active
  - A preferred path only on the preferred controller, then the preferred path on the preferred controller becomes active
  - A preferred path on the non-preferred controller, then one path on the preferred controller becomes active
  - No preferred paths, then one path on the preferred controller becomes active

- If there is no preferred controller and
  - — a preferred path on each controller, then the preferred path on the currently active controller becomes active
  - — a preferred path only on the currently active controller, then the preferred path on that controller becomes active
  - — a preferred path only on the nonactive controller, then the nonactive controller and the preferred path become active
  - — no preferred paths, no change occurs

Syntax:

```
spmgr restore all
             -d device
             -r WWNN
```

spmgr restore all

Restores all LUNs to their preferred paths and/or preferred controller. If you do not have a preferred controller, the default will be the current controller. If you have a preferred path, the default will be the current path.

Syntax:

```
# spmgr restore all
```

Example:

```
# spmgr restore all
```

spmgr restore -d device

Restores a preferred path to the indicated device.

Syntax:

```
# spmgr restore -d device
```

Example:

```
# spmgr restore -d spa
```

spmgr restore -r WWNN

Restores a preferred path to the indicated storage system.

Syntax:

```
# spmgr restore -r WWNN
```

Example:

```
# spmgr restore –r 5000-1FE1-0010-5B00
```

The quiesce command

Quiescing an object means to:

- Move all active I/O from an object to an alternate path.
- Mark all paths to the object as *quiesced* to temporarily remove the object from use.

The objects that are supported for v3.0C of Secure Path are adapters and controllers. Also, quiescing individual paths is supported to allow other fabric infrastructure, such as switches, to be removed and replaced.

Note: Path verification is not performed on a quiesced path.

Syntax:

```
# spmgr quiesce-a HBA
          -c controller_serial_number
          -p path_instance
```

spmgr quiesce -a HBA

When this command is invoked, `spmgr` will move all active I/O using this HBA to paths available on other HBAs. The paths of the specified HBA will then be marked as *quiesced,* and no further I/O will be sent along that path until the HBA is returned to service with the corresponding restart command.

These actions may be verified by issuing the `# spmgr display -a HBA` command to view the current path state.

Use this feature to move I/O to another adapter as the first step to replacing an HBA.

Example:

```
# spmgr quiesce -a 2300-1
```

spmgr quiesce -c controller_serial_number

When this command is invoked, `spmgr` moves all active I/O using this controller to paths on the other controller of the storage system. The paths of the specified controller will then be marked as *quiesced,* and no further I/O will be sent along that path until the controller is returned to service with the restart command.

These actions may be verified by issuing the `# spmgr display -c` *`controller`* command to view the current path states.

Use this feature to move I/O to the other controller as the first step to upgrading or replacing a controller.

Example:

```
# spmgr quiesce -c P56350A91MN19M
```

spmgr quiesce -p path_instance

When this command is invoked, `spmgr` moves all active I/O using this path to another path on the same controller, if possible, or to a path on the `other` controller. The specified path will then be marked as *quiesced,* and no further I/O will be sent along that path until the path is returned to service with the restart command.

These actions may be verified by issuing the `spmgr display` command to view the current path states.

Example:

```
# spmgr quiesce -p hsx_mod-1-0-0-2
```

The restart command

Object restarting changes a quiesced adapter, controller, or path to an *Available* or *Standby* state. When restarted, the HBA or controller is available as an I/O entity for a path.

Syntax:

```
# spmgr restart all
          -a HBA
          -c controller
          -p path_instance
```

spmgr restart all

When this command is invoked, `spmgr` verifies the existence of all components on quiesced paths and changes those paths to *Available* or *Standby* as appropriate. If the Auto-Restore feature is enabled and one or more of those paths are Preferred paths, those paths will be made the Active path.

spmgr restart -a HBA

When this command is invoked, `spmgr` verifies the existence of the HBA and then changes the state of the paths using the HBA to *Available* or *Standby*. If the Auto-Restore feature is enabled and a path using that HBA is the preferred path, the path will be made the *Active* path.

Example:

```
# spmgr restart -a 2300-0
```

spmgr restart -c controller

When invoked, `spmgr` verifies the existence of the controller and then changes the state of the paths using the controller to *Standby*. If the Auto-Restore feature is enabled and a path using that controller is the preferred path, then the path is made the *Active* path.

Example:

```
# spmgr restart -c fire-top
```

spmgr restart -p path_instance

When invoked, `spmgr` verifies the existence of the path and then changes the state of the path to *Available* or *Standby*. If the Auto-Restore feature is enabled and the path is the *Preferred* path, the path will be made *Active*.

Example:

```
# spmgr restart -p hsx-mod_1-0-0-2
```

The passwd Command

Secure Path requires authentication before running commands to ensure that only authorized individuals have access to your storage environment. Use the `passwd` command to change the default password to a unique password.

spmgr passwd agent_password

To enter a new password, use the following `spmgr passwd` command.

Syntax:

```
spmgr passwd <new password>
```

Note: After running this command, you must stop and restart the agent using `spagent -k` to stop and `spagent` to start.

Removing/Upgrading Secure Path

5

This chapter describes how to remove or update Secure Path software. The following topics are covered:

Removing Secure Path software

This section describes how to remove the Secure Path using the Red Hat Package Management (RPM) utility.

1. Unmount all Secure Path file systems before you remove Secure Path.
2. Choose the appropriate option to remove Secure Path v3.0C:

   For 32-bit machines:

   — To remove Secure Path v3.0C for Linux or Secure Path v3.0C for Linux Workgroup Edition, enter a command similar to the following:

   ```
   # rpm -e Secure-Path-3.0C<Full or wkgrp>-<rev>
   ```

   For example:

   ```
   # rpm -e Secure-Path-3.0CFull-4.0
   ```

   For 64-bit machines:

   — To remove Secure Path v3.0C for Linux or Secure Path v3.0C for Linux Workgroup Edition, enter a command similar to the following:

   ```
   # rpm -e Secure-Path-3.0C<Full or wkgrp>64-<rev>
   ```

   For example:

   ```
   # rpm -e Secure-Path-3.0Cwkgrp64-4.0
   ```

   — To remove Secure Path v3.0C for Linux or Secure Path v3.0C for Linux Workgroup Edition on IA64 SUSE/UnitedLinux, enter a command similar to the following:

   ```
   # rpm -e Secure-Path-3.0C<Full or wkgrp>UL64-<rev>
   ```

   For example:

   ```
   # rpm -e Secure-Path-3.0CFullUL64-4.0
   ```

   For either Secure Path for Linux v3.0C or Secure Path v3.0C for Linux Workgroup Edition, the following specific operating system output displays:

   For SUSE/UnitedLinux operating systems:

   ```
   Found boot.swsp file.
   Removing boot.swsp file.
   Removal of Secure Path complete.
   Please reboot system to unload Secure Path modules.
   ```

For Red Hat operating systems:

```
Insertion point found in /etc/rc.d/rc.sysinit
Removal of Secure Path complete.
Please reboot system to unload Secure Path modules.
```

Note: If the RAID storage system is to be used for single-path access by one or more servers, then the HSG80 dual-redundant controllers must be restored to Transparent Failover mode. Refer to "HSG80 Controller Failover Transitions" on page 105 to perform the transition to Transparent Failover mode.

Refer to MSA1000 documentation to set MSA1000 to single-path mode.

Updating to Secure Path for Linux v3.0C

The following sections describe the update rpms and requirements for 32-bit or 64-bit operating systems.

32-bit systems

The system is not required to have previous versions of Secure Path (v3.0, v3.0A, or v3.0B) installed for the update to succeed. However, Secure Path v3.0, v3.0A, or v3.0B RPM must be located in the `/tmp/securepathRPM` directory so the update can be validated.

To update from Secure Path v3.0, v3.0A, or v3.0B to Secure Path v3.0C, ensure that you have the following in the `/tmp/securepathRPM` directory:

Table 10: Secure Path v3.0C 32-bit update RPMs

For this Secure Path version:	Use:
Secure-Path-3.0BFull-5.0.noarch.rpm	Secure-Path-3.0CFullUpdate
Secure-Path-3.0Bc-5.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate
Secure-Path-3.0AFull-4.0.noarch.rpm	Secure-Path-3.0CFullUpdate
Secure-Path-3.0Ac-4.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate
Secure-Path-3.0-8.0.noarch.rpm	Secure-Path-3.0CFullUpdate
Secure-Path-3.0c-8.0.noarch.rpm	Secure-Path-3.0CwkgrpUpdate

64-bit systems

If you are updating from Secure Path v3.0B (for Linux or Linux Workgroup) to Secure Path v3.0C (for Linux or Linux Workgroup), you can access the update kit at the following web site:

http://h18000.www1.hp.com/products/sanworks/secure-path/index.html.

The system is not required to have Secure Path v3.0B, installed for the update to succeed. However, the Secure Path v3.0C RPM must be located in the `/tmp/securepathRPM` directory so the update can be validated.

Table 11 lists the update RPMs for 64-bit systems in this release of Secure Path:

Table 11: Secure Path v3.0C 64-bit update RPMs

For this operating system:	To update this RPM:	Use:
Red Hat	Secure-Path-3.0BFull64-4.0.noarch.rpm	Secure-Path-3.0CFull64Update
Red Hat	Secure-Path-3.0Bc64-4.0.noarch.rpm	Secure-Path-3.0Cwkgrp64 Update
SUSE/ UnitedLinux	Secure-Path-3.0BFullSuse64-4.0.noarch.rpm	Secure-Path-3.0CFullUL64 Update
SUSE/ UnitedLinux	Secure-Path-3.0BcSuse64-4.0.noarch.rpm	Secure-Path-3.0CwkgrpUL64 Update

Note: For SUSE/United Linux rpms, the rpm name has changed from **FullSuse64** to **FullUL64**.

Note: Because there is no commercial update process at this time for updating Red Hat Enterprise Linux 2.1 to Red Hat Enterprise Linux 3.0, or for updating SUSE LINUX 7/UnitedLinux 1.0 to SUSE LINUX 8/UnitedLinux 1.0, you must follow the update procedures described in either "32-bit systems" on page 96 or "64-bit systems" on page 96.

- Updating these systems requires a complete installation, which wipes out everything on the hard disk.
- If a previous version of Secure Path is installed, the update solution saves all configuration files and then updates the Secure Path software to v3.0C.

Updating the software

This update procedure addresses both Secure Path v3.0C for Linux and Secure Path v3.0C for Linux Workgroup Edition. The Secure Path v3.0C for Linux update kit is available on the HP web site at

http://h18000.www1.hp.com/products/sanworks/secure-path/index.html

Use the following steps to update Secure Path:

1. Ensure that the Secure Path v3.0C top level directory includes:
   - `Readme` file
   - `./update_SPlinuxFull.sh` and `./update_SPlinuxwkgrp.sh`
   - rpm files reside in `RPM` directory
2. Choose the appropriate command to update Secure Path:
   - For Secure Path v3.0C, enter:

     ```
     ./update_SPlinuxFull.sh
     ```

   - For Secure Path v3.0C Workgroup Edition, enter:

     ```
     ./update_SPlinuxwkgrp.sh
     ```

Note: Do not use `rpm -Uvh` to update the software. The installation will fail.

The following example shows update instructions and message displays from the update installer:

Example:

```
Welcome to the Secure Path Linux 3.0C update installer.
============================================================


IMPORTANT: You must have a valid copy of the
Secure-Path-3.0-8.0.noarch.rpm or
Secure-Path-3.0AFull-4.0.noarch.rpm or
Secure-Path-3.0BFull-5.0.noarch.rpm
Secure-Path-3.0BFull64-4.0.noarch.rpm or
Secure-Path-3.0BFullUL64-4.0.noarch.rpm in the
/tmp/securepathRPM directory to validate the update!!!
============================================================
```

— If you have an unsupported kernel version, the following message displays:

```
************************************************************

The kernel on this system is not supported. Please see
documentation for supported kernel versions.
Exiting.....

************************************************************
```

— If you are not running smp or an enterprise kernel. The following message displays:

```
************************************************************

SMP or enterprise kernel must be loaded to install this kit.
Exiting.....

************************************************************
```

— If the kernel is supported, the following message displays:

```
This is a supported kernel. Continuing with the
installation.
```

— For 32-bit SUSE/UnitedLinux with a proper kernel version of 2.4.21-169-smp, the following error message displays:

```
************************************************************

The system is not running the kernel (2.4.21-169-smp).

Would you like to install anyway? [y/N]

************************************************************
```

— For 64-bit SUSE/UnitedLinux with a proper kernel version of 2.4.21-112-itanium2-smp, the following error message displays:

```
************************************************************

The system is not running kernel (2.4.21-112-itanium2-smp).

Would you like to install anyway? [y/N]

************************************************************
```

— For 32-bit or 64-bit Red Hat 3.0 with a non-supported errata version, but with a proper kernel version of 2.4.21-9.ELsmp, the following error message displays:

```
************************************************************

The system is not running the errata kernel(2.4.21-9.ELsmp).
The system is not running a supported errata kernel.

Would you like to install anyway? [y/N]

************************************************************
```

— For 32- bit Red Hat 2.1 with a non-supported errata version, but with a proper kernel version of 2.4.9-e.35smp, the following error message displays:

```
************************************************************

The system is not running the errata kernel (2.4.9-e.35smp).
The system is not running a supported errata kernel.

Would you like to install anyway? [y/N]

************************************************************
```

— For 64-bit Red Hat 2.1 with a non-supported errata version, but with a proper kernel version of 2.4.18-e.41-smp, the following error message displays:

```
************************************************************

The system is not running errata kernel (2.4.18-e.41smp).
The system is not running a supported errata kernel.

Would you like to install anyway? [y/N]

************************************************************
```

If you choose **N** or **n**, the following message displays and the installation ends:

```
You have chosen not to continue. Exiting...
```

— The installation script checks for previous versions of Secure Path. If there is no instance of a Secure Path v3.x installation, the following message displays:

```
You do not currently have an installation of secure path.
```

If Secure Path is installed, a message similar to the following displays:

```
RPM: Secure-Path-3.0BFull-5.0 is installed.
```

OR:

```
RPM: Secure-Path-3.0Bc-5.0 is installed.
```

The installation script then checks in the `/tmp/securepathRPM` directory. For example:

```
Secure-Path-3.0Bc-5.0.noarch.rpm
```

The following message displays:

```
Checking for rpm...
```

— If this installation script cannot find the rpm, an appropriate installation type message displays, as shown in the following examples:

For Secure Path v3.0 for Linux:

```
*******************************************************

Secure-Path-3.0-8.0.noarch.rpm was not found in the
/tmp/securepathRPM.
Secure Path Linux 3.0 to 3.0C update unavailable on this
system.
Checking for valid update path from Secure Path Linux 3.0A to
3.0C...

*******************************************************
```

For Secure Path v3.0A for Linux Workgroup Edition:

```
*************************************************************


Secure-Path-3.0AFull-4.0.noarch.rpm was not found in the
/tmp/securepathRPM.
Secure Path Linux 3.0A to 3.0C update unavailable on this
system.
Checking for valid update path from Secure Path Linux 3.0B to
3.0C...

*************************************************************
```

For Secure Path v3.0B for Linux:

```
*************************************************************

Secure-Path-3.0Bc-5.0.noarch.rpm was not found in
the/tmp/securepathRPM.
Secure Path Linux 3.0B to 3.0C update unavailable on this
system.
Requirements not met to update Secure Path. Please see
documentation for update requirements

*************************************************************
```

— If the installation can find a previous version of the rpm, a message similar to the following examples displays:

For Secure Path v3.0B for Linux:

```
Found an instance of Secure-Path-3.0BFull-4.0.noarch.rpm.
```

For Secure Path v3.0B for Linux Workgroup Edition:

```
Found an instance of Secure-Path-3.0Bc-4.0.noarch.rpm.
```

— The RPM update continues with the following message:

```
This script will update Secure Path, saving important
configuration files and restoring them upon completion.
Note, that the current installation will be removed!!!

Would you like to update Secure Path?

Note: Current installation of Secure Path will be
uninstalled! [y/N]
```

— If you choose `N`, the following message displays and the installation ends:

```
You have chosen not to continue.  Exiting…
```

— If you choose `y`, and there was a previous installation of Secure Path, the following message displays:

```
Saving configuration files…

Removing previous installation…
```

The installation script executes a `rpm -e` on the previous installation of Secure Path. Refer to "Removing Secure Path software" on page 94 for `rpm -e` output.

— When the `rpm -e` has finished executing, the script takes over and the following message displays:

```
Installing Secure Path…
```

At this point the script executes an `rpm -ivh` or an `rpm -ivh --force` on the `rpm` to install it. Refer to "Installing Secure Path" on page 45 for information on unsupported kernel error messages.

— If an rpm is found in the `/tmp/securepathRPM` directory, the following message displays:

```
Checking validity of RPM...
```

— You may receive a message similar to the following if you have a valid Secure Path rpm in the `/tmp/securepathRPM` directory:

```
Secure Path 3.0B Full RPM validated continuing with
update!!!
```

— If you do not have a valid Secure Path rpm, a message similar to the following examples displays:

32-bit Example:

```
************************************************************

INVALID RPM:

You must have a valid Secure-Path-3.0BFull-5.0.noarch.rpm in
the /tmp/securepathRPM directory, to validate the update!!!
Update failed.
Exiting...

************************************************************
```

64-bit Example:

```
************************************************************

INVALID RPM:

You must have a valid Secure-Path-3.0BFull64-4.0.noarch.rpm
in the /tmp/securepathRPM directory, to validate the
update!!!
Update failed.
Exiting...

************************************************************
```

— If the rpm finishes successfully and there was a previous installation of Secure Path, the following message displays:

```
Copying saved configuration files to /etc/CPQswsp/…
```

— If the rpm does not finish successfully and there was a previous installation of Secure Path, the following message displays:

```
/etc/CPQswsp directory not found, configuration files will
not be copied.  Installation did not finish successfully
Configuration files are saved in /tmp/spholddir.
```

HSG80 Controller Failover Transitions

This appendix describes how to set dual-redundant HSG80 controllers from one failover state to another. The failover states are Transparent Failover, Multiple-bus Failover, and No Failover. The following topics are covered:

Establishing a serial connection to the controller

Before changing failover states, you must establish a serial connection to the controller as follows:

1. Establish a serial connection to the controller with the serial line connected to the top controller.

   This controller will be referred to as `this_controller`. The second controller will be referenced as the `other_controller`. All HSG80 actions in the next steps are assumed to be through this serial connection.

2. Verify the current state of the controllers by entering:

   ```
   CLI> show this_controller
   ```

   The display from the `show` command has a number of sections. The information that is required is contained in the first section, with the header of *Controller*. A sample display for Transparent Failover is shown below. The failover state is identified with an arrow `(->)` preceding the noted text.

   ```
   Controller:
           HSG80 ZG83502145 Software V85F-0, Hardware  E03
           NODE_ID          = 5000-1FE1-0000-3350
           ALLOCATION_CLASS = 0
           SCSI_VERSION     = SCSI-3
    ->     Configured for dual-redundancy with ZG80200290
    ->      In dual-redundant configuration
   ```

   As the controller state changes, the display will be shown to help verify that the change has completed successfully.

3. After establishing a serial connection to the controller, choose one of the following types of failover transitions to change the controller states that are described in this appendix.

   — “Changing from Transparent Failover to no failover mode” on page 107

   — “Changing from Transparent Failover to Multiple-bus Failover mode” on page 108

   — “Changing from Multiple-bus Failover mode to no failover and then to Transparent Failover mode” on page 110

Changing from Transparent Failover to no failover mode

1. Enter the following command at the CLI prompt:

   ```
   CLI> set nofailover
   ```

   This action causes the OTHER_CONTROLLER to shut down.

2. Enter the following command to verify the change to no failover.

   ```
   CLI> show this_controller

Controller:
        HSG80 ZG83502145 Software V85F-0, Hardware  E03
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-3
    ->  Not Configured for dual-redundancy
   ```

3. Restart the OTHER_CONTROLLER by pressing the **RESET** button on the OTHER_CONTROLLER.

   The OTHER_CONTROLLER sounds an alarm as it discovers the second controller but detects that it is not bound in a failover mode. You can silence the alarm and disregard the message about the controllers being misconfigured.

   Enter the following command to verify the change in controller state:

   ```
   CLI> show this_controller

Controller:
        HSG80 ZG83502145 Software V85F-0, Hardware  E03
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-3
   ->   Not Configured for dual-redundancy
   ->       Controller misconfigured -- other controller
present
   ```

Note: This state change is important only if a controller is to be replaced, or if the state is changing from Transparent Failover to Multiple-bus Failover or vice-versa. This is not an ending state in itself.

Changing from Transparent Failover to Multiple-bus Failover mode

Regardless of whether you have defined UNITs for the RAID system, the following steps implement Transparent Failover to Multiple-bus Failover.

1. Enter the following command at the CLI prompt:

   ```
   CLI> set nofailover
   ```

   This action causes the OTHER_CONTROLLER to shut down.

2. Enter the following command at the CLI prompt to verify the change to *no failover*:

   ```
   CLI> show this_controller

   Controller:
           HSG80 ZG83502145 Software V85F-0, Hardware  E03
           NODE_ID          = 5000-1FE1-0000-3350
           ALLOCATION_CLASS = 0
           SCSI_VERSION     = SCSI-3
    ->     Not Configured for dual-redundancy
   ```

3. Restart the OTHER_CONTROLLER by pressing the **RESET** button on the OTHER_CONTROLLER.

   The OTHER_CONTROLLER will sound an alarm as it discovers the second controller but detects that it is not bound in Failover mode. You can silence the alarm and disregard the message about the controllers being misconfigured.

   ```
   Controller:
   HSG80 ZG83502145 Software V85F-0, Hardware  E03
   NODE_ID          = 5000-1FE1-0000-3350
   ALLOCATION_CLASS = 0
   SCSI_VERSION     = SCSI-3
   -> Not Configured for dual-redundancy
   -> Controller misconfigured -- other controller present
   ```

4. When the OTHER_CONTROLLER is online, enter the following command to place the controllers into Multiple-bus Failover mode:

   ```
   CLI> set multibus_failover copy=this_controller
   ```

   This action copies all unit and connection information to the OTHER_CONTROLLER and restarts both controllers.

After both controllers have restarted, the controller pair will be bound in Multiple-bus Failover mode with consistent views of all the RAID array information.

5. Verify that the controllers are now in Multiple-bus Failover:

```
CLI> show this_controller

Controller:
        HSG80 ZG83502145 Software V85F-0, Hardware  E03
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-3
    ->  Configured for MULTIBUS_FAILOVER with ZG80200290
    ->      In dual-redundant configuration
```

6. If the RAID array had connections prior to making this transition, examine the connections by entering the following command:

```
CLI> show connections
```

7. Inspect the last column, `offset value`, by entering the following command.

```
CLI> set connection connection_name unit_offset=0
```

Note: In Transparent Failover mode, the controller, by default, assigns an offset value of 0 to the left-hand port and an offset value of 100 to the right-hand port. In Multiple-bus Failover mode, the controller assigns an offset value of 0 to all ports, unless existing connections have nonzero offset values.

Changing from Multiple-bus Failover mode to no failover and then to Transparent Failover mode

1. Check for connections on the storage system. For HSG80 controllers, enter the following command:

   ```
   CLI> show connections
   ```

2. Delete all connections by entering the following command for each connection that is shown (if any):

   ```
   CLI> delete connection_name
   ```

Note: The connections will be regenerated later.

---

3. Check for units on the storage system:

   ```
   CLI> show units
   ```

4. Delete all units by entering the following command for each unit (Dn) that is shown (if any):

   ```
   CLI> delete dn
   ```

Note: The UNITs will be restored after the controller state is changed. HP recommends that you record Dn values and associated information, as well as the storageset information, for later use. The controller state change will not affect the data on the storagesets.

---

5. If the controllers are currently in a failover mode, enter the following command to shut down the OTHER_CONTROLLER:

   ```
   CLI> set nofailover
   ```

6. Verify the current state of the controller, by entering the following command:

   ```
   CLI> show this_controller
   ```

```
Controller:
        HSG80 ZG83502145 Software V85F-0, Hardware  E03
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-3
   ->   Not Configured for dual-redundancy
```

7. Restart the OTHER_CONTROLLER by pressing the **RESET** button on the OTHER_CONTROLLER.

   The OTHER_CONTROLLER will sound an alarm as it discovers the second controller but detects that it is not bound in a failover mode. You can silence the alarm and disregard the message about the controllers being misconfigured.

   Verify the current state of the controller by entering the following command:

   ```
   CLI> show this_controller
   ```

   ```
   Controller:
           HSG80 ZG83502145 Software V85F-0, Hardware  E03
           NODE_ID          = 5000-1FE1-0000-3350
           ALLOCATION_CLASS = 0
           SCSI_VERSION     = SCSI-3
      ->   Not Configured for dual-redundancy
   -> Controller misconfigured -- other controller present
   ```

8. When the OTHER_CONTROLLER is available, enter the following command to copy all unit and configuration information to the OTHER_CONTROLLER and restart it:

   ```
   CLI> set failover copy=this_controller
   ```

9. Verify the controller state by entering the following command. When restarted, the controller pair will be bound in Transparent Failover mode.

   ```
   CLI> show this_controller
   ```

   ```
   Controller:
           HSG80 ZG83502145 Software V85F-0, Hardware  E03
           NODE_ID          = 5000-1FE1-0000-3350
           ALLOCATION_CLASS = 0
           SCSI_VERSION     = SCSI-3
       ->  Configured for dual-redundancy with ZG80200290
       ->      In dual-redundant configuration
   ```

10. Restore the UNIT to the storageset mapping that was recorded earlier by entering the following command:

```
CLI> add unit dn storage_set_name
```

Caution: Do not initialize the storagesets. This action will destroy data on the storagesets.

11. Restart both controllers by entering the following commands:

```
CLI> restart other_controller
CLI> restart this_controller
```

Note: Restarting both controllers allows connections to be reacquired. You can also accomplish this by rebooting the servers.

Fibre Channel Device Software

B

This chapter describes Secure Path persistence software. The following topics are covered:

Using Secure Path Persistence Software

Linux SCSI layer overview

The Linux operating system does not provide built-in LUN persistence. Lack of LUN persistence means that if you add or delete physical LUNs or disks and reboot your system, there is a probability that the device mnemonics will change in an undesirable way. Table 12 shows a system with three LUNs displayed:

Table 12: System displaying three LUNs

Device name	Bus-Target-LUN	Disk content
/dev/sda	Bus 0 Target 0 LUN 0	System disk
/dev/sdb	Bus 0 Target 0 LUN 1	Obsolete data
/dev/sdc	Bus 0 Target 0 LUN 2	New data

In this example, `/dev/sdb` is not needed anymore and needs to be removed. So, the disk is unmounted and removed. At some point, the system is rebooted and failed to mount `/dev/sdc` the *new data* disk.

Upon further analysis, the system now thinks that *new data* disk is `/dev/sdb`. This situation occurs frequently, due to the way physical buses are scanned and device mnemonics are bound to them.

When the system is first booted, the buses are scanned for devices in the order by which they are detected. Devices are scanned on a bus starting at LUN 0 and up. Device mnemonics are assigned in order starting with `sda` until all the major/minor numbers are exhausted.

Because `/dev/sdb` was deleted from the system, on the next boot, `/dev/sdc` was reassigned to `/dev/sdb`. This is not desirable behavior.

Persistence defined

Persistence is the binding of a device mnemonic to a physical device regardless of the device's location on the bus.

Persistence is a very important concept, especially in Fibre Channel topologies. In a Fibre Channel fabric, devices come and go much the same way network attached devices, such as PCs, connect to and disconnect from a LAN. Normally, you will install a disk, create a filesystem on it, and mount it.

The next time you boot the system, the expectation is that your disk device mnemonics won't change because some neighboring device was added, removed, or set offline.

The `sps` program maintains persistence through the use of symbolic links. The `sps` program is meant to be run at boot time just after the Secure Path modules are loaded. To that end, the Secure Path installation process adds execution of `sps` to one of the system boot files. You never need to execute `sps` manually.

The sps program conclusion

Secure Path for Linux uses the `sps` program for maintaining device persistence. The program does the following:

- Reads in a list of associations it knows about (physical -> logical -> symbolic).
- Reads in a list of physical devices the hardware indicates is present at that time.
- Compares the above and does the following:
  - — Makes symbolic links for new devices.
  - — Deletes symbolic links for nonexistent devices.
  - — Modifies symbolic links to compensate for physical device movement to another bus and/or another target or LUN.

The symbolic links are maintained in `/dev/spdev.` Links are created for all partitions of the LUN. Therefore, you will see `/dev/spdev/spa` through `dev/spdev/spa15` where `spa` represents `spa0.`

Having stated that, here are the issues using persistence and the `sps` program.

It is possible to fill the `sps` data file in which case the program will fail to do its job. The reason for this is built into the technology of persistence itself.

With a Fibre Channel Network, devices may go offline. That does not mean that they're gone for good. It does mean that they're not available right now. In order to ensure persistence, `sps` must remember the device. It is possible over time to fill the table with devices that may never come back online.

If this happens and a genuine new device is added, there will be no room to add it to the data file and `sps` fails.You must edit the persistence data file to remove unneeded entries because the Linux SCSI layer is currently limited to 128 LUNs.

Editing full Persistence data files

The `sps` persistence data file is located at `/etc/CPQswsp/sppf.` You can tell if the file is full by entering `wc -l /etc/CPQswsp/sppf` and looking at the line count. If it's 128 lines, you cannot add more LUNs. You can add new LUNs only if you delete existing LUNs from the `sppf` file. It is possible that some of the LUNs in the `sppf file` are no longer used.

Using a standard editor

Note: Create a backup copy of the file prior to opening the `sppf` file.

Using the editor of your choice, open the `/etc/CPQswsp/sppf` file and delete the lines that correspond to LUNs that are no longer available. Make sure you delete the entire line.

Note: Editing a line is not recommended; doing so could corrupt your database and render it useless.

After you have deleted the lines for non-existent LUNs, save and close the file.

When you reboot the system, `/etc/CPQswsp/bin/sps` runs and the new persistence entries are added.

Summary of sps features and limitations

The important points about the `sps` for Secure Path v3.0C for Linux program are as follows:

- Runs at boot time, normally.
- Creates symbolic links in `/dev/spdev`, which should be used in place of the normal device driver files.
- Tracks a device between reboots even if device moves to another bus or slot.
- Can fill up persistence data file to a maximum of 128 LUNs.
- Persistence data file may contain LUN information for LUNs that will never return.
- Editing out stale LUNs in the `sppf` data file is the only way to free slots for new LUNs.

glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

Controller

A controller is a hardware device that facilitates communication between a host and one or more LUNs organized as an array. The HSG80, HSV110, HSV100 and MSA1000 controllers are supported for use with Secure Path.

Controller States

- **Critical—**Reported for a controller pair bound in Multiple-bus Failover mode when only one of the controllers is available. This state may mean a failed or offline condition, since the server cannot communicate with the other controller at this time.
- **Operational—**The controller is available with a good status.
- **Unknown—**The server cannot communicate with this controller.

Device States

Attributes that describe the current operational condition of a device. A device may exist in the following states:

- **Critical—**Only one path remains available to the storage unit.
- **Degraded—**At least one or more paths are failed to the storage unit.
- **Operational—**The Secure Path device can be accessed on at least one path.
- **Unknown—**Unable to communicate with the unit. This may indicate no available path or a failed device.
- **Dead—**All paths used by this Secure Path device have failed.

Fabric

A network comprised of high-speed fiber connections resulting from the interconnection of switches and devices. A fabric is an active and intelligent non-shared interconnect scheme for nodes.

HBA
A Host Bus Adapter is an I/O device that serves as the interface connecting a host system to the SAN (Storage Area Network).

LUN
A Logical Unit Number is the actual unit number assigned to a device at the RAID system controller.

Object
The objects that are supported for v3.0C of Secure Path are adapters and controllers.

Path
A virtual communication route that enables data and commands to pass between a host server and a storage device.

Path States and Attribute

- **Active—**Currently used for the I/O stream.
- **Available—**Available on the active controller for the I/O stream.
- **Failed—**Currently unusable for the I/O stream.
- **Quiesced—**Path is valid but the user has moved all I/O from it.
- **Standby—**The path is valid on the standby controller.
- **Preferred—**A path that is preferred for the I/O stream, across reboots.

Port A
The relative number of an HBA. A specific port number is determined according to its order of discovery by the Windows operating system and includes SCSI, Fibre Channel, and IDE adapter types.

SAN
Storage Area Network. A configuration of networked devices for storage.

State
State is an attribute that describes the current operational condition of an object. See Path, Path States and Attribute, Controller States, and Device States.

index

A

C

O

P

Q

R

S

T

U

V

W